EP ・ US

特 許 協 力 条 約

PCT

国際調査報告

（法８条、法施行規則第40、41条）
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人 の書類記号 ５２２１９６ＷＯ０１	今後の手続きについては、国際調査報告の送付通知様式（ＰＣＴ／ＩＳＡ／２２０）及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ００／０９１２９	国際出願日 （日.月.年） ２２．１２．００	優先日 （日.月.年） １４．０１．００
出願人（氏名又は名称） 三菱電機株式会社		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で 3 ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第 1 図とする。☒ 出願人が示したとおりである。 ☐ なし
☐ 出願人は図を示さなかった。
☐ 本図は発明の特徴を一層よく表している。

国際調査報告

国際出願番号 PCT／JP00／09129

A. 発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷ H04L9／10

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷ H04L9／10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP, 9－298736（松下電器産業株式会社） 18. 11月. 1997（18. 11. 97） 第10頁右欄第28行目～第12頁左欄第31行目，全図 （ファミリーなし）	1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, 41-44

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 30. 03. 01	国際調査報告の発送日 10.04.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木 重徳　印　5W　2956 電話番号 03－3581－1101 内線 3535

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP，10－123950，A（富士ゼロックス株式会社） 15．5月．1998（15．05．98） 第4頁右欄第38行目～第5頁左欄第27行目，第21図	8, 10, 18, 20, 24, 26, 30, 32, 34, 36, 38, 40, 45-50
A	全文，全図 ＆　EP，837383，A2　＆　US，6161183，A	9, 19, 25, 31
X	JP，8－248879，A（インターナショナル・ビジネス・マシーンズ・コーポレイション） 27．9月．1996（27．09．96） 第4頁右欄第33行目～第43行目，全図 ＆　EP，725511，A2 ＆　US，5673319，A1	8-10, 18-20, 24-26, 30-32, 34, 36, 38, 40, 45-50
A	JP，4－48336，A（富士通株式会社） 18．2月．1992（18．02．92） 全文，全図（ファミリーなし）	1-50
A	JP，2－73747，A（日本電気株式会社） 13．3月．1990（13．03．90） 全文，第1図（ファミリーなし）	1-50
A	JP，57－69344，A（日本電信電話公社） 28．4月．1982（28．04．82） 全文，全図（ファミリーなし）	1-50
A	JP，4－191935，A（株式会社東芝） 10．7月．1992（10．07．92） 全文，全図　（ファミリーなし）	1-50

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2001年7月19日 (19.07.2001)

PCT

(10) 国際公開番号
WO 01/52472 A1

(51) 国際特許分類[7]: H04L 9/10

(21) 国際出願番号: PCT/JP00/09129

(22) 国際出願日: 2000年12月22日 (22.12.2000)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-5161 2000年1月14日 (14.01.2000) JP

(71) 出願人 (米国を除く全ての指定国について): 三菱電機株式会社 (MITSUBISHI DENKI KABUSHIKI KAISHA) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 反町 亨 (SORIMACHI, Toru) [JP/JP]. 時田俊雄 (TOKITA, Toshio) [JP/JP]; 〒100-8310 東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内 Tokyo (JP).

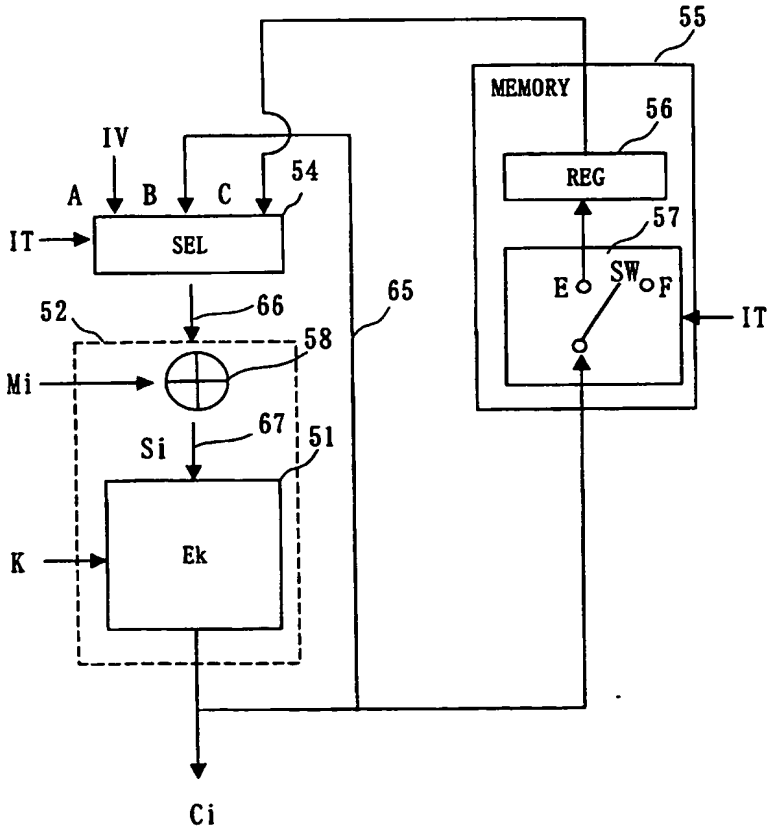
(74) 代理人: 溝井章司, 外(MIZOI, Shoji et al.); 〒247-0056 神奈川県鎌倉市大船二丁目17番10号 NTA大船ビル 3F Kanagawa (JP).

(81) 指定国 (国内): AU, CA, CN, JP, KR, MX, NO, SG, US.

[続葉有]

(54) Title: METHOD AND APPARATUS FOR ENCRYPTION, METHOD AND APPARATUS FOR DECRYPTION, AND COMPUTER-READABLE MEDIUM STORING PROGRAM

(54) 発明の名称: 暗号化装置及び暗号化方法及び復号装置及び復号方法及びプログラムを記録したコンピュータ読み取り可能な記録媒体



(57) Abstract: In order to encipher data while enciphering other data, a memory (55) is arranged in parallel to a feedback line (65) for feedback to a selector (54) from an enciphering module (51) using an encryption key (K). If an interrupt (IT) for processing plaintext block data (N_i) occurs during the processing of plaintext block data (M_i), the cryptogram block data (C_i) being in process when the interrupt (IT) occurs is stored in a register (56). When the processing of the plaintext block data N_i is completed, a selector (54) selects the cryptogram block data (C_i) stored in the memory (55), and the processing of plaintext block data (M_i+1) is started.

[続葉有]

WO 01/52472 A1

(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

(57) 要約:

暗号化の最中に他のデータの暗号化を行うために、暗号鍵Ｋを用いた暗号化モジュール５１からセレクタ５４にフィードバックするフィードバックライン６５に対して並列に設けられたメモリ５５を配置する。平文ブロックデータM_i を処理中に他のデータの平文ブロックデータN_i を処理する割り込みＩＴが発生した場合には、割り込みＩＴが発生したときの暗号文ブロックデータC_i をレジスタ５６に記憶させ、平文ブロックデータN_i の処理が終了した時点でメモリ５５に記憶した暗号文ブロックデータC_i をセレクタ５４に選択させることにより平文ブロックデータM_{i+1} の処理を開始する。

明　細　書

暗号化装置及び暗号化方法及び復号装置及び復号方法及びプログラムを記録したコンピュータ読み取り可能な記録媒体

技術分野

この発明は、暗号化復号装置及び暗号化復号方法に関するものである。特に、データの暗号化復号の最中に他のデータの暗号化復号ができる発明に関するものである。

背景技術

図４３は、Ｃｉｐｈｅｒ　Ｂｌｏｃｋ　Ｃｈａｉｎｉｎｇ　Ｍｏｄｅ（以下、ＣＢＣモードという）による暗号化装置を示す図である。

図４３に示すＣＢＣモードでの暗号方法は、６４ビットの平文ブロックデータM_iをブロック単位で入力して、暗号鍵Ｋを用いた暗号化モジュール５１により暗号化し、更に、この暗号化された暗号文ブロックデータC_iと次の平文ブロックデータM_{i+1}との排他的論理和を演算し、排他的論理和の演算結果を次の暗号化の入力として、暗号鍵Ｋを用いた暗号化モジュール５１に供給することにより暗号化する方法である。そして、この処理を繰り返して次々と連鎖させることにより、平文Ｍ全体を暗号文Ｃに暗号化するものである。

図４４は、ＣＢＣモードを用いた復号装置を示す図である。

図４４に示す復号装置は、図４３に示す暗号化装置により暗号化された暗号文を復号する装置である。暗号文ブロックデータC_1が暗号鍵Ｋを用いた復号モジュール７１に入力され、イニシャルバリューＩＶとの排他的論理和が計算され、平文ブロックデータM_1が復号される。暗号

文ブロックデータC_2が入力された場合には、暗号鍵Kを用いた復号モジュール７１で復号され、先に入力され、レジスタ１１１に保存された暗号文ブロックデータC_1との排他的論理和がとられ、平文ブロックデータM_2を復号する。

なお、レジスタ１１１は、セレクタ７３の内部に設けられていてもよい。

平文ブロックデータをM_i（i＝1，2，・・・，n）、暗号文ブロックデータC_i（i＝1，2，・・・，n）とし、暗号鍵Kを用いた暗号化処理をE_K、暗号鍵Kを用いた復号処理をD_Kとすると、ＣＢＣモードは次式で表される。

$C_1 = E_K (M_1 \text{ EXR } IV)$

$C_i = E_K (M_i \text{ EXR } C_{i-1})$ （i＝2，3，・・・，n）

$M_1 = D_K (C_1) \text{ EXR } IV$

$M_i = D_K (C_i) \text{ EXR } C_{i-1}$ （i＝2，3，・・・，n）

ここで、ＥＸＲは排他的論理和演算である。また、ＩＶ（Ｉｎｔｉａｌ　Ｖａｌｕｅ）は初期値であり、最初の暗号化と復号の際に用いられる。イニシャルバリューＩＶは、暗号化側と復号側で同一の値を用いる。

図４５は、Ｏｕｔｐｕｔ　Ｆｅｅｄｂａｃｋ　Ｍｏｄｅ（以下、ＯＦＢモードという）の暗号化装置を示す図である。

図４６は、ＯＦＢモードの復号装置を示す図である。

図４７は、Ｃｉｐｈｅｒ　Ｆｅｅｄｂａｃｋ　Ｍｏｄｅ（以下、ＣＦＢモードという）の暗号化装置を示す図である。

図４８は、ＣＦＢモードの復号装置を示す図である。

なお、レジスタ１１１は、セレクタ７３の内部に設けられていてもよい。

図４９は、ＣＢＣモードの暗号化装置を用いて平文Ｍと平文Ｎを暗号化する手順を示す図である。

ここでは、平文Ｍが平文ブロックデータM_1，平文ブロックデータM_2，平文ブロックデータM_3から構成されており、平文Ｎが平文ブロックデータN_1のみで構成されている場合を説明する。

平文ブロックデータM_1の暗号化がスタートすると、暗号文ブロックデータC_1が出力されるとともに、暗号文ブロックデータC_1は、平文ブロックデータM_2の暗号化に用いられる。このように、暗号文ブロックデータC_iは、平文ブロックデータM_{i+1}の暗号化にフィードバックされて連鎖処理が行われる。従って、平文ブロックデータM_1から平文ブロックデータM_3までの暗号化が終わらなければ、平文ブロックデータN_1の暗号化を行うことができない。

図５０は、図４９と同様に、ＣＢＣモードで暗号化を行う場合を示している。

図５０の場合は、平文ブロックデータM_1、平文ブロックデータM_2、平文ブロックデータM_3の各データが準備されるのに時間がかかってしまう場合を示している。一方、暗号化処理は、次の平文ブロックデータM_{i+1}が準備できる前に終了しており、アイドル時間（例えば、Ｔ１～Ｔ２、Ｔ３～Ｔ４の時間）が発生してしまう場合を示している。このように、アイドル時間が発生する場合でも、暗号文ブロックデータC_iが次の平文ブロックデータM_{i+1}にフィードバックされる連鎖処理を行わなければならないため、平文ブロックデータN_1の処理は平文ブロックデータM_3の処理が終了してからでなければ行えない。

図５１は、データの秘匿処理とデータの完全性を保証する処理を示す図である。平文Ｍは、例えば、ＯＦＢモードの暗号装置により暗号文Ｃに暗号化される。ＣＢＣモードの暗号装置により認証子Ｐが演算され、

暗号文Ｃの最後に認証子Ｐが付加される。暗号化され、かつ、認証子Ｐが付加されたデータを受信した場合には、暗号文Ｃから平文ＭをＯＦＢモードの復号装置により復号するとともに、暗号文ＣからＣＢＣモードの復号装置により認証子Ｐを演算し、伝送されてきた認証子Ｐと同一か否かを比較することにより、伝送されてきたＣが改竄されていないことを確認することができる。

図５２は、図５１に示した秘匿処理と認証子演算処理の手順を示す図である。

平文ブロックデータM_1～平文ブロックデータM_3は、順に暗号文ブロックデータC_1～暗号文ブロックデータC_3に暗号化される。その後、暗号文ブロックデータC_1～暗号文ブロックデータC_3を順に入力して認証子Ｐが演算される。

図４２～図４８に示した各モードの暗号化装置及び復号装置は、前のブロックデータの暗号化復号されたデータをフィードバックさせて次のブロックデータの暗号化復号処理に利用しなければならないため、一旦暗号化処理又は復号処理がスタートしてしまうと、その全体の処理が終了しない限り、他の暗号化処理又は復号処理をスタートさせることができないという課題があった。従って、先にスタートした暗号化復号処理が長時間要するものである場合には、後からスタートする暗号化復号処理が長時間待たされてしまうという課題があった。

また、暗号化復号されるデータが準備される時間に比べて、暗号化復号処理に要する時間が短い場合には、暗号化復号化装置にアイドル時間が発生してしまうという課題があった。

また、秘匿処理と完全性保証処理を行う場合には、秘匿処理を行ってから完全性保証処理を行わなければならず、処理時間がかかってしまうという課題があった。

この発明の好適な実施の形態においては、あるデータの暗号化復号処理の最中に他のデータの暗号化復号処理を行える暗号化装置、復号装置及び暗号化方法及び復号方法を得ることを目的とする。

また、この発明の好適な実施の形態においては、優先度の高いデータの暗号化復号を優先的に行えるようにすることを目的とする。

また、この発明の好適な実施の形態においては、秘匿処理と完全性保証処理を並列的に高速に行えるようにすることを目的とする。

発明の開示

この発明に係る暗号化装置は、第１の処理データと、第２の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第１の処理データの暗号化処理が完了する前に第２の処理データの暗号化処理を開始するとともに、第２の処理データの暗号化処理を開始する場合に第１の処理データの暗号化処理の状態を上記メモリに記憶させ、第１の処理データの暗号化処理を再開する場合に、暗号化装置の暗号化処理の状態を、メモリに記憶した第１の処理データの暗号化処理の状態に復帰させてから第１の処理データの暗号化処理を再開することを特徴とする。

上記暗号化装置は、第２の処理データの暗号処理の完了する前に第１の処理データの暗号化処理を再開するとともに、上記メモリは、第１の処理データの暗号化処理を再開する場合に第２の処理データの暗号化処理状態を記憶し、第２の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態を、メモリに記憶した第２の処理データの暗号化処理の状態に復帰させてから第２の処理データの暗号化処理を再

開することを特徴とする。

上記第１の処理データは、第１の平文であり、上記第２の処理データは、第２の平文であることを特徴とする。

上記暗号化装置は、割り込みにより第２の処理データの暗号化処理を開始することを特徴とする。

この発明に係る暗号化装置は、平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、

平文Ｍの暗号化処理中に平文Ｎの暗号化要求を平文Ｍの暗号化処理完了前に受け付けるメカニズムと、

平文ブロックデータM_iの暗号化処理を行い暗号文ブロックデータC_iを出力する暗号化ユニットと、

暗号化ユニットから出力された暗号文ブロックデータC_iをフィードバックラインを介し暗号化ユニットにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータC_iを記憶するメモリと、

平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン

によりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループに供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶された暗号文ブロックデータC_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする。

この発明に係る暗号化方法は、暗号化モジュールから出力される暗号文ブロックデータC_i（i＝1，2，3，・・・）を用いて第1の平文Mの平文ブロックデータM_i（i＝1，2，3，・・・）を暗号化する工程と、

上記平文ブロックデータM_iを暗号化している途中で又は平文ブロックデータM_iを暗号化した後に、第1の平文Mの平文ブロックデータM_{i+1}の暗号化に用いられる暗号文ブロックデータC_iをメモリに記憶する工程と、

上記平文ブロックデータM_{i+1}の暗号化に用いられる暗号文ブロックデータC_iをメモリに記憶した後に、第2の平文Nの少なくとも1つの平文ブロックデータを暗号化する工程と、

上記第2の平文Nの少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータM_{i+1}の暗号化に用

いられる暗号文ブロックデータC_iを入力し、暗号化モジュールを用いて第１の平文Mの平文ブロックデータM_{i+1}を暗号化する工程と
を備えたことを特徴とする。

この発明に係る暗号化装置は、１つ以上の平文ブロックデータからなる平文を暗号化ユニット暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータC_iを暗号化ユニットへフィードバックする第１のフィードバックループを有し、平文ブロックデータを入力し、第１のフィードバックループにより暗号文ブロックデータC_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と
を備えたことを特徴とする。

上記暗号化部と認証子生成部とは、１つの暗号化モジュールと、１つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと
を備えたことを特徴とする。

この発明に係る暗号化方法は、１つ以上の平文ブロックデータからなる平文を暗号化ユニットにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータC_iを暗号化ユニットへフィードバックする第１のフィードバック工程を有し、平文ブロックデータを入力し、第１のフィードバックループにより暗号文ブロックデータC_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と
を備えたことを特徴とする。

この発明に係る復号装置は、第１の処理データと、第２の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

第１の処理データの復号処理が完了する前に第２の処理データの復号処理を開始するとともに、第２の処理データの復号処理を開始する場合

に第１の処理データの復号処理の状態を上記メモリに記憶させ、第１の処理データの復号処理を再開する場合に、復号装置の復号処理の状態を、メモリに記憶した第１の処理データの復号処理の状態に復帰させてから第１の処理データの復号処理を再開することを特徴とする。

上記復号装置は、第２の処理データの復号処理の完了する前に第１の処理データの復号処理を再開するとともに、上記メモリは、第１の処理データの復号処理を再開する場合に第２の処理データの復号処理状態を記憶し、第２の処理データの復号処理を再開する場合は、復号装置の復号処理の状態を、メモリに記憶した第２の処理データの復号処理の状態に復帰させてから第２の処理データの復号処理を再開することを特徴とする。

上記第１の処理データは、第１の暗号文であり、上記第２の処理データは、第２の暗号文であることを特徴とする。

上記復号装置は、割り込みにより第２の処理データの最初のブロックデータの復号処理を開始することを特徴とする。

この発明に係る復号装置は、暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータD_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、

暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付けるメカニズムと、

暗号文ブロックデータC_iの復号処理を行い平文ブロックデータM_i

を出力する復号ユニットと、

暗号文ブロックデータC_{i+1}を復号するための暗号文ブロックデータC_iをフィードバックラインを介し復号ユニットにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Dの復号要求を受け付け、暗号文Dのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされる暗号文ブロックデータC_iを記憶するメモリと、

暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループに供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Dのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶された暗号文ブロックデータC_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチとを備えたことを特徴とする。

この発明に係る復号方法は、復号モジュールを用いて第１の暗号文Cの暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）を復号する工

程と、

上記暗号文ブロックデータC_iを復号している途中で又は暗号文ブロックデータC_iを復号した後に、第１の暗号文Ｃの暗号文ブロックデータC_{i+1}の復号に用いられる暗号文ブロックデータC_iをメモリに記憶する工程と、

上記暗号文ブロックデータC_{i+1}の復号に用いられる暗号文ブロックデータC_iをメモリに記憶した後に、第２の暗号文Ｄの少なくとも１つの暗号文ブロックデータを復号する工程と、

上記第２の暗号文Ｄの少なくとも１つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータC_{i+1}の復号に用いられる暗号文ブロックデータC_iを入力し、復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_{i+1}を復号する工程と

を備えたことを特徴とする。

この発明に係る復号装置は、１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータT_iを復号モジュールへフィードバックする第１のフィードバックループを有し、暗号文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し

、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と
を備えたことを特徴とする。

上記復号部と認証子生成部とは、１つの復号モジュールと、１つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと
を備えたことを特徴とする。

この発明に係る復号方法は、１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータT_iを復号モジュールへフィードバックする第１のフィードバック工程を有し、暗号文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程

を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

この発明に係る暗号化装置は、平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、

平文Ｍの暗号化処理中に平文Ｎの暗号化要求を平文Ｍの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行ったデータをモジュール出力ブロックデータT_iとして出力する暗号化モジュールと、

暗号化モジュールから出力されたモジュール出力ブロックデータT_iをフィードバックラインを介し暗号化モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされるモジュール出力ブロックデータT_iを記憶するメモリと、

平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン

によりフィードバックされるモジュール出力ブロックデータT_iを選択してフィードバックループに供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたモジュール出力ブロックデータT_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする。

この発明に係る暗号化方法は、暗号化モジュールから出力されるモジュール出力ブロックデータT_i（i＝1，2，3，・・・）を用いて第1の平文Mの平文ブロックデータM_i（i＝1，2，3，・・・）を暗号化する工程と、

上記平文ブロックデータM_iを暗号化している途中で又は平文ブロックデータM_iを暗号化した後に、第1の平文Mの平文ブロックデータM_{i+1}の暗号化に用いられるモジュール出力ブロックデータT_iをメモリに記憶する工程と、

上記平文ブロックデータM_{i+1}の暗号化に用いられるモジュール出力ブロックデータT_iをメモリに記憶した後に、第2の平文Nの少なくとも1つの平文ブロックデータを暗号化する工程と、

上記第2の平文Nの少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータM_{i+1}の暗号化に用

いられるモジュール出力ブロックデータT_iを入力し、暗号化モジュールを用いて第１の平文Mの平文ブロックデータM_{i+1}を暗号化する工程と

を備えたことを特徴とする。

この発明に係る暗号化装置は、１つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータT_iを暗号化モジュールへフィードバックする第１のフィードバックループを有し、平文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備えたことを特徴とする。

上記暗号化部と認証子生成部とは、１つの暗号化モジュールと、１つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモ

リと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする。

この発明に係る暗号化方法は、１つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータT_iを暗号化モジュールへフィードバックする第１のフィードバック工程を有し、平文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

この発明に係る復号装置は、暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータD_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、

暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行ったデータをモジュール出力ブロックデータT_iとして出力する復号モジュールと、

復号モジュールから出力されたモジュール出力ブロックデータT_iをフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Ｄの復号要求を受け付け、暗号文Ｄのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされるモジュール出力ブロックデータT_iを記憶するメモリと、

暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるモジュール出力ブロックデータT_iを選択してフィードバックループに供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Ｄのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたモジュール出力ブロックデータT_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする。

上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする。

この発明に係る復号方法は、復号モジュールから出力されるモジュール出力ブロックデータT_i（i＝1，2，3，・・・）を用いて第1の暗号文Cの暗号文ブロックデータC_i（i＝1，2，3，・・・）を復号する工程と、

上記暗号文ブロックデータC_iを復号している途中で又は暗号文ブロックデータC_iを復号した後に、第1の暗号文Cの暗号文ブロックデータC_{i+1}の復号に用いられるモジュール出力ブロックデータT_iをメモリに記憶する工程と、

上記暗号文ブロックデータC_{i+1}の復号に用いられるモジュール出力ブロックデータT_iをメモリに記憶した後に、第2の暗号文Dの少なくとも1つの暗号文ブロックデータを復号する工程と、

上記第2の暗号文Dの少なくとも1つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータC_{i+1}の復号に用いられるモジュール出力ブロックデータT_iを入力し、復号モジュールを用いて第1の暗号文Cの暗号文ブロックデータC_{i+1}を復号する工程と

を備えたことを特徴とする。

この発明に係る復号装置は、1つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータC_iを復号ユニットへフィードバックする第1のフィードバックループを有し、暗号文ブロックデータを入力し、第1のフィードバックループにより暗号文ブロックデータC_iをフィードバ

ックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

を備えたことを特徴とする。

上記復号部と認証子生成部とは、１つの復号モジュールと、１つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと

を備えたことを特徴とする。

この発明に係る復号方法は、１つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

暗号文ブロックデータC_iを復号ユニットへフィードバックする第１のフィードバック工程を有し、暗号文ブロックデータを入力し、第１のフィードバックループにより暗号文ブロックデータC_iをフィードバッ

クさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

を備えたことを特徴とする。

上記暗号化処理は、ブロック暗号アルゴリズムを用いることを特徴とする。

上記復号処理は、ブロック暗号アルゴリズムを用いることを特徴とする。

上記メモリは、暗号化処理の状態として、

第１の処理データの暗号化途中結果と、

第１の処理データを暗号化するために用いる暗号鍵と

を記憶することを特徴とする。

上記メモリは、復号処理の状態として、

第２の処理データの復号途中結果と、

第２の処理データを復号するために用いる復号鍵と

を記憶することを特徴とする。

この発明に係る暗号化装置は、データを入力して暗号化し、暗号デー

タを出力する暗号化部と、

暗号化部が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備え、

認証子生成部は、暗号化部によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする。

この発明に係る復号装置は、データを入力して復号し、復号データを出力する復号部と、

復号部が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備え、

認証子生成部は、復号部によるデータの復号が完了する前に認証子の生成を開始することを特徴とする。

この発明に係る暗号化方法は、データを入力して暗号化し、暗号データを出力する暗号化工程と、

暗号化工程が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備え、

認証子生成工程は、暗号化工程によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする。

この発明に係る復号方法は、データを入力して復号し、復号データを出力する復号工程と、

復号工程が入力したデータを入力して暗号文の完全性を保証するため

の認証子を生成する認証子生成工程と

を備え、

認証子生成工程は、復号工程によるデータの復号が完了する前に認証子の生成を開始することを特徴とする。

また、この発明は、上記暗号化装置の各部の処理及び上記暗号化方法の各工程の処理をコンピュータに実行させるためのプログラムであることを特徴とする。また、そのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

また、この発明は、上記復号装置の各部の処理及び上記復号方法の各工程をコンピュータに実行させるためのプログラムであることを特徴とする。また、そのプログラムを記録したコンピュータ読み取り可能な記録媒体であることを特徴とする。

図面の簡単な説明

図１は、実施の形態１のＣＢＣモードの暗号化装置を示す図。

図２は、ＣＢＣモードの暗号化装置の動作手順を示す図。

図３は、ＣＢＣモードの暗号化装置の動作フローチャート図。

図４は、セレクタ５４の動作フローチャート図。

図５は、スイッチ５７の割り込み処理フローチャート図。

図６は、メモリ５５の他の例を示す図。

図７は、メモリ５５の割り込み処理フローチャート図。

図８は、メモリ５５の他の例を示す図。

図９は、優先度処理を示す図。

図１０は、優先度処理を示す図。

図１１は、優先度処理を示す図。

図１２は、メモリ５５がフィードバックライン６６と並列に設けられている図。

図１３は、図１２の暗号化装置の動作手順を示す図。

図１４は、メモリ５５がフィードバックライン６７に並列に設けられている図。

図１５は、図１４の暗号化装置の動作手順を示す図。

図１６は、ＯＦＢモードの暗号化装置を示す図。

図１７は、図１６の暗号化装置の動作手順を示す図。

図１８は、ＣＦＢモードの暗号化装置を示す図。

図１９は、図１８の暗号化装置の動作手順を示す図。

図２０は、ＣＢＣモードの復号装置を示す図。

図２１は、図２０の復号装置の動作手順を示す図。

図２２は、ＯＦＢモードの復号装置を示す図。

図２３は、図２２の復号装置の動作手順を示す図。

図２４は、ＣＦＢモードの復号装置を示す図。

図２５は、図２４の復号装置の動作手順を示す図。

図２６は、鍵を保存するＣＢＣモードの暗号化装置を示す図。

図２７は、ＣＢＣモードの暗号化装置の動作手順を示す図。

図２８は、鍵を保存するＣＢＣモードの復号装置を示す図。

図２９は、実施の形態２の暗号化部１００と認証子生成部２００を有する暗号化装置を示す図。

図３０は、暗号化部１００と認証子生成部２００を有する暗号化装置の動作手順を示す図。

図３１は、暗号化部１００と認証子生成部２００を有する暗号化装置のフローチャート図。

図３２は、暗号化部１００と認証子生成部２００を１つにした暗号化装置を示す図。

図３３は、暗号化部１００と認証子生成部２００を１つにした暗号化装置の動作手順を示す図。

図３４は、復号化部３００と認証子生成部４００を有する復号装置を示す図。

図３５は、復号化部３００と認証子生成部４００を１つにした復号装置を示す図。

図３６は、復号化部３００と認証子生成部４００を１つにした復号装置の動作手順を示す図。

図３７は、実施の形態２の暗号化部１００と認証子生成部２００を有する暗号化装置を示す図。

図３８は、復号化部３００と認証子生成部４００を有する復号装置を示す図。

図３９は、暗号鍵Ｋを用いた暗号化モジュール５１の代表的構成図。

図４０は、暗号化装置及び復号装置のハードウェア実現例を示す図。

図４１は、暗号化装置及び復号装置のハードウェア実現例を示す図。

図４２は、アプリケーションプログラム４６により暗号化プログラム４７が呼び出される場合を示す図。

図４３は、従来のＣＢＣモードの暗号化装置を示す図。

図４４は、従来のＣＢＣモードによる復号装置を示す図。

図４５は、従来のＯＦＢモードの暗号化装置を示す図。

図４６は、従来のＯＦＢモードによる復号装置を示す図。

図４７は、従来のＣＦＢモードの暗号化装置を示す図。

図４８は、従来のＣＦＢモードによる復号装置を示す図。

図４９は、従来の暗号化手順を示す図。

図５０は、従来の暗号化手順を示す図。

図５１は、秘匿処理と完全性保証処理を説明する図。

図５２は、従来の秘匿処理と完全性保証処理の動作手順を示す図。

発明を実施するための最良の形態

実施の形態１.

図１は、この実施の形態におけるＣＢＣモードの暗号化装置を示す図である。

この実施の形態の暗号化装置は、セレクタ５４と排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１とメモリ５５とにより構成されている。排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１とは、暗号化ユニット５２を構成している。セレクタ５４と排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１は、フィードバックライン６５とフィードバックライン６６とフィードバックライン６７によりフィードバックループを構成している。暗号鍵Ｋを用いた暗号化モジュール５１により暗号化された暗号文ブロックデータC_iは、フィードバックループにより再び排他的論理和回路５８に入力され、排他的論理和回路５８でモジュール入力データS_iが生成される。そして、生成されたモジュール入力データS_iが暗号鍵Ｋを用いた暗号化モジュール５１に供給される。

メモリ５５は、フィードバックライン６５と並列に設けられている。メモリ５５は、レジスタ５６とスイッチ５７により構成されている。スイッチ５７は、暗号鍵Ｋを用いた暗号化モジュール５１の出力をレジスタ５６に入力させるか無視するかを切り替えるものである。この切り替えは、例えば、割り込みＩＴにより行われる。割り込みＩＴが発生した場合には、スイッチ５７はＥに接続され、割り込みＩＴが解除された場

合には、スイッチ５７はＦに接続される。レジスタ５６は、Ｅを経由してきた暗号文ブロックデータC_iを入力して記憶するものである。レジスタ５６に記憶された暗号文ブロックデータC_iは、セレクタ５４に出力される。セレクタ５４は、Ａ，Ｂ，Ｃの３つの入力を有しており、いずれか１つの入力を選択するものである。これらの選択は、後述するように割り込みＩＴに依存する。

図２は、図１に示した暗号化装置の動作手順を示す図である。

図３は、図１に示した暗号化装置の動作フローチャートである。

この暗号化装置が電源を投入された場合のセレクタ５４の入力はＡに設定されており、スイッチ５７はＥに接続されているものとする。また、平文Ｎの暗号化要求があるときは、割り込みＩＴが発生し、平文Ｎの暗号化要求が解除されるまで、割り込みＩＴがオンになり続けるものとする。また、平文Ｍは、鍵K_1を用いて暗号化され、平文Ｎは、鍵K_2を用いて暗号化されるものとする。また、割り込みＩＴが発生したとき又は割り込みＩＴが解除されたときには、鍵K_2又は鍵K_1が暗号化モジュール５１に支給され直すものとする。

時刻Ｔ０において、鍵K_1が支給され、平文ブロックデータM_1の暗号化処理がスタートする。時刻Ｔ０において、平文ブロックデータM_1の暗号化がスタートした場合には、セレクタ５４の入力Ａから一旦イニシャルバリューＩＶが入力された後、セレクタ５４はＢに切り替わる。そして、平文ブロックデータM_1が鍵K_1を用いて暗号化されている途中の時刻Ｘにおいて、平文ブロックデータN_1の暗号化を要求する割り込みＩＴが発生したとする。時刻Ｔ１までに、暗号文ブロックデータC_1はメモリ５５に記憶された状態になる。そして、割り込みＩＴの発生により時刻Ｔ１において、鍵K_2が暗号化モジュール５１に支給される。また、時刻Ｔ１において、セレクタ５４は入力をＡに設定する。また

、時刻Ｔ１において、スイッチ５７はＦに接続される。時刻Ｔ１以降は、鍵K_2を用いて平文ブロックデータN_1の暗号化が行われ、暗号文ブロックデータD_1が出力される。時刻Ｙにおいて、平文ブロックデータN_1の暗号化が終了し、割り込みＩＴが解除されたものとする。この割り込みＩＴの解除により時刻Ｔ２において、鍵K_1が暗号化モジュール５１に支給され、セレクタ５４の入力はＣに切り替えられ、スイッチ５７はＥに接続される。セレクタ５４がＣに切り替わったことにより、メモリ５５に記憶されていた暗号文ブロックデータC_1が平文ブロックデータM_2の暗号化のために入力され、鍵K_1を用いた暗号化モジュール５１により平文ブロックデータM_2が暗号化されて、暗号文ブロックデータC_2が出力される。時刻Ｔ３以前においては、セレクタ５４の入力はＢに切り替えられ、平文ブロックデータM_3を暗号化する場合には、フィードバックループのフィードバックライン６５からフィードバックされた暗号文ブロックデータC_2が入力され、鍵K_1を用いた暗号化モジュール５１により平文ブロックデータM_3暗号化されて、暗号文ブロックデータC_3が出力される。

なお、平文Ｍと平文Ｎの鍵が同一（$K_1 = K_2$）の場合は、鍵は暗号処理のスタート時に一度だけ供給されればよい。

図３のフローチャートを用いて全体の動作を説明する。

Ｓ１において、平文Ｍの暗号化処理がスタートし続行される。最後のブロックデータまで処理を終えた場合には、処理を終了する。Ｓ２において、任意の時点で生じる割り込みＩＴの発生が監視される。割り込みＩＴの発生がない場合には、Ｓ１の処理が続行される。平文ブロックデータM_iの処理中に割り込みＩＴが発生した場合には、Ｓ３において、現在処理中の平文ブロックデータM_iの暗号文ブロックデータC_iをメモリ５５のレジスタ５６に記憶する。Ｓ４において、割り込みＩＴによ

り暗号化処理の要求があった平文Ｎの暗号化処理を行う。このＳ４の暗号化処理は、Ｓ５に示すように、割り込みＩＴの解除があるまで連続して行われる。割り込みＩＴの解除があった場合には、Ｓ６において、メモリ５５のレジスタ５６に記憶した暗号文ブロックデータC_iを用いてM_{i+1}の暗号化処理を行う。それ以降の処理は、Ｓ１に戻り、暗号化処理が続行される。

図４は、セレクタ５４のオペレーション処理を示す図である。

電源がオンになった場合には、Ｓ１１に示すように、入力をＡに設定する。Ｓ１２において、暗号化がスタートした場合には、Ｓ１３において、入力をＢに設定する。即ち、フィードバックループのフィードバックライン６５によりフィードバックされる暗号文ブロックデータC_iが用いられる。Ｓ１４において、現在処理しているブロックデータが最後であるということが判定された場合には、Ｓ１１に戻り電源オンと同じ状態に戻る。Ｓ１５において、割り込みＩＴの発生が確認された場合には、Ｓ１６において、入力をＡに設定し、暗号化がスタートした場合には、Ｓ１８において、入力をＢに設定する。割り込みＩＴの解除があるまでは、入力がＢに設定されたままで動作する。即ち、フィードバックループのフィードバックライン６５によりフィードバックされる暗号文ブロックデータC_iが用いられる。Ｓ１９において、割り込みＩＴの解除があったことが検知された場合には、Ｓ２０において、入力をＣに設定する。この入力をＣに設定することにより、メモリ５５に記憶された暗号文ブロックデータC_iが入力されることになる。このＣからの入力による暗号化がスタートした場合には、Ｓ１３に戻り入力をＢに設定する。

このようにして、割り込みＩＴの発生に基づき、セレクタ５４を切り替えることができる。

なお、平文Mの暗号化処理も、割り込みＩＴにより任意の時刻にスタートさせてもよい。

図５は、スイッチ５７の割り込み処理のフローチャートである。

電源がオンになった場合、そして、その後の最初の平文の暗号化処理の場合は、スイッチ５７はＥに接続される。そして、Ｓ３１において、割り込みＩＴが発生した場合には、スイッチ５７をＥからＦに接続する。そして、Ｓ３３において、割り込みＩＴの解除が検出された場合には、スイッチ５７をＦからＥに接続する。このようにして、スイッチ５７は、割り込みＩＴの発生から解除までは暗号文ブロックデータC_iを無視する。従って、メモリ５５のレジスタ５６には、割り込みＩＴが発生したときに生成された暗号文ブロックデータC_iが記憶され続けることになる。

以上のように、図１～図５に示した暗号化装置は、平文Mを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、平文Mの暗号化処理中に平文Ｎの暗号化要求を平文Mの暗号化処理完了前に受け付ける割り込み処理メカニズムを示している。

また、図１～図５に示した暗号化装置は、平文ブロックデータM_iの暗号化処理を行い、暗号文ブロックデータC_iを出力する暗号化モジュール５１と、暗号化モジュール５１から出力された暗号文ブロックデータC_iをフィードバックライン６５を介し暗号化ユニット５２にフィードバックするフィードバックループ６５，６６と、フィードバックループのフィードバックライン６５と並列に設けられ、上記割り込み処理により上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデー

タM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータC_iを記憶するメモリ５５とを有している。

また、図１～図５に示した暗号化装置は、平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン６５によりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループを介して暗号化ユニット５２に供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Ｎのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリ５５に記憶された暗号文ブロックデータC_iを選択してフィードバックループを介して暗号化ユニット５２に供給するセレクタ５４を有している。

メモリ５５は、割り込みＩＴが発生したときの暗号化装置の状態を記憶するメモリである。メモリ５５が暗号化処理の状態を記憶しておくことにより、あるデータの暗号化の最中に他のデータの暗号化を行った場合でも、再びあるデータの暗号化の処理に復帰することができる。即ち、メモリ５５に記憶されたデータを用いることにより、暗号化が中断されたときと全く同じ状態に暗号化装置を復帰させることができ、中断した暗号化処理を続行させることが可能になる。

図６は、メモリ５５の他の例を示す図である。

メモリ５５は、割り込み制御部５２と入力スイッチ９６と出力スイッチ９７と複数のレジスタ（ＲＥＧ１，２，３）を有している。このように、複数のレジスタを有することにより、複数の割り込みを受け付けることが可能になる。

図７は、メモリ５５の割り込み処理の動作を示す図である。

割り込みＩＴが発生すると、Ｓ４１において、現在使用中のレジスタ

kの番号kを記憶する。Ｓ４２において、入力スイッチ９６と出力スイッチ９７をレジスタk以外のレジスタ１に接続する。この状態で、平文Ｎの暗号化が継続される。更に、平文Ｎの暗号化の最中に他の割り込みが発生したかを監視する。Ｓ４３において、他の割り込みＩＴが発生したことが検出された場合には、再び自分自身であるＳ４０の処理を呼び出す。このように、割り込みＩＴが発生するたびに、自分自身をＳ４０の処理をリカーシブに呼び出すことにより、複数階層の割り込み処理を行うことができる。Ｓ４４においては、割り込みが解除されたかを検出し、割り込みが解除された場合には、入力スイッチ９６と出力スイッチ９７を記憶しておいた番号kを用いてレジスタkに切り替える。図６に示す場合は、３つのレジスタがあるので、３階層の割り込み処理を行うことができる。

図８は、メモリ５５の他の例を示す図である。

メモリ５５は、スタック６４を有している。スタック６４は、先入れ後出し（ＦＩＬＯ）のレジスタである。スタック１を使用中に割り込みＩＴが発生した場合には、スタック１のデータをスタック２に移し、それ以後のデータをスタック１に積み上げ、割り込みＩＴが解除された場合には、積み上げたスタック１のデータを出力し、スタック２のデータをスタック１に戻す。図８に示す場合は、４階層の割り込み処理を行える場合を示している。

図６に示すように、複数階層の割り込み処理を行うことができる場合は、各割り込みに対して優先度を付けることができる。例えば、割り込みＩＴ１を優先度１とし、割り込みＩＴ２を優先度１より優先度の低い優先度２とすることにより、優先度１の割り込みＩＴ１が発生した場合には、優先度２の処理を遅らせることができる。

図９は、優先度１の暗号化処理を優先度２の暗号化処理に優先させた

場合を示している。優先度１の暗号化処理を先に終了させている。

図１０は、優先度がともに等しい場合の暗号化処理の場合を示している。

優先度が等しい場合には、２つの平文の各ブロックデータを交互に暗号化する。

図１１は、優先度１のデータと２つの優先度２のデータを暗号化する場合を示している。

図９～図１１に示すように、割り込みに優先度を付けることによりユーザが望ましいと思われる暗号化処理手順を実現することができる。緊急用のデータや短いデータの場合には、優先度を高くすることにより効率のよい処理を行うことができる。

図１２は、メモリ５５をフィードバックライン６６と並列においた場合を示している。

排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１とは、暗号化ユニット５２を構成している。

図１３は、図１２の暗号化装置の動作手順を示す図である。

第１セレクタ６１と第２セレクタ６２とは、以下のような選択接続により、図１のセレクタ５４と同じ選択動作をさせるものである。

第１のセレクタ６１＋第２のセレクタ６２＝セレクタ５４

A	＋	D	＝	A
B	＋	D	＝	B
A	＋	C	＝	C
B	＋	C	＝	C

図１３では、第２のセレクタ６２がＤを選択しているときは、第１のセレクタ６１の選択（Ａ又はＢ）が有効となり、第２のセレクタ６２がＣを選択しているときは、メモリ５５の内容が出力されることになる。

即ち、第２のセレクタ６２は、メモリ５５の内容を用いたいとき（割り込みＩＴが解除されて平文Ｎから元の平文Ｍへの暗号化に戻るとき）に、Ｃを選択すればよい。

図１４は、メモリ５５をフィードバックライン６７と並列においた場合を示している。

図１５は、図１４の暗号化装置の動作手順を示す図である。

割り込みＩＴが発生した時刻Ｘが排他的論理和回路５８で排他的論理和演算される前である場合には、メモリ５５は、排他的論理和回路５８により排他的論理和演算されたモジュール入力データS_iを記憶する。そして、平文ブロックデータN_1を暗号化する。次に、メモリ５５に記憶されたモジュール入力データS_iを第２セレクタ６２により選択させ、暗号鍵Ｋを用いた暗号化モジュール５１に入力し、暗号化して暗号文ブロックデータC_1を出力する。

図１及び図１２及び図１４に示すように、メモリ５５は、フィードバックライン６５とフィードバックライン６６とフィードバックライン６７のいずれのラインと並列の設けられていても構わない。メモリ５５は、暗号化装置が、あるデータの暗号化処理中に他のデータの暗号化を開始するとき、他のデータの暗号化を開始する直前の状態を覚えておくものであり、他のデータの暗号化処理が終了した時点で、メモリ５５に記憶されたデータを用いて暗号化装置が元の状態に復帰できるのであれば、メモリ５５は、どの場所に設けられていても構わない。また、メモリ５５は、複数箇所に設けられていてもよい。

以上のように、この実施の形態に係る暗号化装置は、１つ以上のブロックデータM_i（ｉ＝１，２，３，・・・，ｍ）からなる第１の処理データ（平文Ｍ）と、１つ以上のブロックデータN_j（ｊ＝１，２，３，・・・，ｎ）からなる第２の処理データ（平文Ｎ）との暗号化処理をす

る暗号化装置において、暗号化処理の状態を記憶するメモリ５５を備え、第１の処理データの全ブロックデータ（M_1 ～M_n ）の暗号化処理が完了する前に第２の処理データの最初のブロックデータN_1 の暗号化処理を開始するとともに、第２の処理データの最初のブロックデータN_1 の暗号化処理を開始する場合に第１の処理データの暗号化処理の状態（例えば、暗号化ブロックデータC_i ）を上記メモリ５５に記憶させ、第１の処理データの暗号化処理を再開する場合に、暗号化装置の暗号化処理の状態を、メモリに記憶した第１の処理データの暗号化処理の状態に復帰させてから第１の処理データの暗号化処理を再開することを特徴とする。

また、上記暗号化装置は、第２の処理データの全ブロックデータ（N_1 ～N_n ）の暗号処理の完了する前に第１の処理データの暗号化処理を再開するとともに、上記メモリ５５は、第１の処理データの暗号化処理を再開する場合に第２の処理データの暗号化処理状態（例えば、暗号化ブロックデータD_j ）を記憶し、第２の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態を、メモリに記憶した第２の処理データの暗号化処理の状態に復帰させてから第２の処理データの暗号化処理を再開することを特徴とする。

図１６は、ＯＦＢモードの暗号化装置の構成図である。

図４５に比べて、メモリ５５が追加されている点が特徴である。メモリ５５は、暗号化モジュール５１から出力されたモジュール出力データT_1 を記憶するものである。

図１６は、平文Ｍを構成する平文ブロックデータM_i （ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j （ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、平文Ｍの暗号化処理中に平文Ｎの暗号化要求を平文Ｍの暗号化処理完了前に受け付ける割

り込み処理メカニズムと、暗号化処理を行ったデータをモジュール出力ブロックデータT_iとして出力する暗号化モジュール５１と、暗号化モジュール５１から出力されたモジュール出力ブロックデータT_iをフィードバックライン６５を介し暗号化モジュールにフィードバックするフィードバックループ６５，６６と、フィードバックループのフィードバックライン６５と並列に設けられ、上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされるモジュール出力ブロックデータT_iを記憶するメモリ５５と、平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン６５によりフィードバックされるモジュール出力ブロックデータT_iを選択してフィードバックループを介して暗号化モジュール５１に供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Ｎのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリ５５に記憶されたモジュール出力ブロックデータT_iを選択してフィードバックループを介して暗号化モジュール５１に供給するセレクタ５４とを備えたことを特徴とする。

図１７は、図１６のＯＦＢモードの暗号化装置の動作説明図である。

図１７は、図２のＣＢＣモードの動作がＯＦＢモードの動作になったものであり、その他の動作は図２の動作と同じである。

図１８は、ＣＦＢモードの暗号化装置を示す図である。

図４７に比べて、メモリ５５が設けられている点が特徴である。メモリ５５は、排他的論理和回路５８から出力された暗号文ブロックデータC_iを記憶するものである。

また、排他的論理和回路５８と暗号鍵Ｋを用いた暗号化モジュール５１とは、暗号化ユニット５２を構成している。

図１８は、平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、平文Ｍの暗号化処理中に平文Ｎの暗号化要求を平文Ｍの暗号化処理完了前に受け付ける割り込み処理メカニズムと、平文ブロックデータM_iの暗号化処理を行い暗号文ブロックデータC_iを出力する暗号化ユニット５２と、暗号化モジュールから出力された暗号文ブロックデータC_iをフィードバックライン６５を介し暗号化処理にフィードバックするフィードバックループ６５，６６と、フィードバックループのフィードバックライン６５と並列に設けられ、上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータC_iを記憶するメモリ５５と、平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックライン６５によりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループを介して暗号化ユニット５２に供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Ｎのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリ５５に記憶された暗号文ブロックデータC_iを選択してフィードバックループを介して暗号化ユニット５２に供給するセレクタ５４とを備えたことを特徴とする。

図１９は、図１８のＣＦＢモードの暗号化装置の動作説明図である。

図１９は、図２のＣＢＣモードの動作がＣＦＢモードの動作になった

ものであり、その他の動作は図２の動作と同じである。

図２０は、ＣＢＣモードの復号装置を示す図である。

図４４に比べて、メモリ７５が設けられている点が特徴である。

メモリ７５は、レジスタ７６とスイッチ７７により構成されている。

また、排他的論理和回路７８と鍵Ｋを用いた復号モジュール７１により復号ユニット７２を構成している。

なお、レジスタ１１１は、セレクタ７４の内部に設けられていてもよい。

図２０に示す復号装置は、暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータN_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付ける割り込み処理メカニズムを有している。

また、図２０に示す復号装置は、暗号文ブロックデータC_iの復号処理を行ったデータをモジュール出力ブロックデータT_iとして出力する復号モジュール７１と、暗号文ブロックデータC_{i+1}を復号するための暗号文ブロックデータC_iをフィードバックライン８５，１１１，８２を介し復号ユニット７２にフィードバックするフィードバックループ８５，１１１，８２，８６と、フィードバックループのフィードバックライン８５，１１１，８２と並列に設けられ、上記暗号文Ｄの復号要求を受け付け、暗号文Ｄのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされるブロックデータを記憶するメモリ７１とを有している。

また、図２０に示す復号装置は、暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバ

ックループのフィードバックライン８５，１１１，８２によりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループを介して暗号ユニット７２に供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Dのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶された暗号文ブロックデータC_iを選択してフィードバックループを介して暗号ユニット７２に供給するセレクタ７４を備えている。

なお、上述した図２０の説明において、「フィードバックライン」、「フィードバックループ」という用語を用いているが、「自己の出力を自己の入力にする」という意味での「フィードバック」ではない。ここでは、「フィードバック」という用語は、暗号文ブロックデータC_iを復号した後に、暗号文ブロックデータC_{i+1}を復号するために、暗号文ブロックデータC_iを再び供給するという意味で用いるものとする。

図２１は、図２０の復号装置の動作手順を示す図である。

暗号鍵（復号鍵ともいう）K_1を用いて、暗号文ブロックデータC_1を復号している最中に割り込みＩＴの発生があった場合には、暗号文ブロックデータC_1がメモリ７５のレジスタ７６に記憶される。その後、暗号鍵（復号鍵ともいう）K_2を用いて、暗号文ブロックデータD_1の復号が行われ、平文ブロックデータN_1が復号される。そして、メモリ７５のレジスタ７６に記憶された暗号文ブロックデータC_1が読み出され、暗号文ブロックデータC_2の復号が行われ、平文ブロックデータM_2が復号される。セレクタ７４の動作は、図４に示したものと同じである。また、スイッチ７７の動作は、図５に示したものと同じである。

図２２は、ＯＦＢモードの復号装置を示す図である。

図２２は、暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータD_j（ｊ

＝１，２，３，・・・）とを復号する復号装置において、暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付ける割り込み処理メカニズムと、復号処理を行ったデータをモジュール出力ブロックデータT_iとして出力する復号モジュール７１と、復号モジュール７１から出力されたモジュール出力ブロックデータT_iをフィードバックライン８５を介し復号モジュール７１にフィードバックするフィードバックループ８５，８６と、フィードバックループのフィードバックライン８５と並列に設けられ、上記暗号文Ｄの復号要求を受け付け、暗号文Ｄのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされるモジュール出力ブロックデータT_iを記憶するメモリ７５と、暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックライン８５によりフィードバックされるモジュール出力ブロックデータT_iを選択してフィードバックループを介して復号モジュール７１に供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Ｄのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリ７５に記憶されたモジュール出力ブロックデータT_iを選択してフィードバックループを介して復号モジュール７１に供給するセレクタ７４とを備えたことを特徴とする。

図２３は、図２２のＯＦＢモードの暗号化装置の動作説明図である。

図２３は、図２１のＣＢＣモードの動作がＯＦＢモードの動作になったものであり、その他の動作は図２１の動作と同じである。

図２４は、ＣＦＢモードの復号装置を示す図である。

また、排他的論理和回路７８と鍵Ｋを用いた復号モジュール７１によ

り復号ユニット７２を構成している。

なお、レジスタ１１１は、セレクタ７４の内部に設けられていてもよい。

図２４は、暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータD_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付ける割り込み処理メカニズムと、暗号文ブロックデータC_iの復号処理を行ったデータをモジュール出力ブロックデータT_iとして出力する復号モジュール７１と、暗号文ブロックデータC_{i+1}を復号するための暗号文ブロックデータC_iをフィードバックライン８５，１１１，８２を介し復号ユニット７２にフィードバックするフィードバックループ８５，１１１，８２，８６と、フィードバックループのフィードバックライン８５，１１１，８２と並列に設けられ、上記暗号文Ｄの復号要求を受け付け、暗号文Ｄのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされる暗号文ブロックデータC_iを記憶するメモリ７５と、暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックライン８５，１１１，８２によりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループを介して復号モジュール７１に供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Ｄのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリ７５に記憶された暗号文ブロックデータC_iを選択してフィードバックループを介して復号モジュール７１に供給するセレクタ７４とを備えたことを

特徴とする。

なお、上述した図２４の説明において、「フィードバックライン」、「フィードバックループ」という用語を用いているが、「自己の出力を自己の入力にする」という意味での「フィードバック」ではない。ここでは、「フィードバック」という用語は、暗号文ブロックデータC_iを復号した後に、暗号文ブロックデータC_{i+1}を復号するために、暗号文ブロックデータC_iを再び供給するという意味で用いるものとする。

図２５は、図２４のＣＦＢモードの暗号化装置の動作説明図である。

図２５は、図２１のＣＢＣモードの動作がＣＦＢモードの動作になったものであり、その他の動作は図２１の動作と同じである。

図２６は、図１に示したＣＢＣモードの暗号化装置の改良例を示す図である。

図２６の暗号化装置は、セレクタ１５４とメモリ１５５とが追加されている。図１の場合は、鍵K_1が割り込みＩＴの解除のとき外部から支給される場合を示したが、ここでは、一度外部から支給された鍵K_1を保存して再利用する場合について説明する。

メモリ１５５は、レジスタ１５６とスイッチ１５７により構成されている。スイッチ１５７は、暗号鍵Ｋをレジスタ１５６に入力させるか無視するかを切り替えるものである。この切り替えは、例えば、割り込みＩＴにより行われる。割り込みＩＴが発生した場合には、スイッチ１５７はＥに接続され、割り込みＩＴが解除された場合には、スイッチ１５７はＦに接続される。レジスタ１５６は、Ｅを経由してきた鍵Ｋを入力して記憶するものである。レジスタ１５６に記憶された鍵Ｋは、セレクタ１５４に出力される。セレクタ１５４は、Ａ，Ｃの２つの入力を有しており、いずれか１つの入力を選択するものである。これらの選択は、後述するように割り込みＩＴに依存する。

図２７は、図２６に示した暗号化装置の動作手順を示す図である。

この暗号化装置が電源を投入された場合のセレクタ５４とセレクタ１５４の入力はＡに設定されており、スイッチ５７とスイッチ１５７はＥに接続されているものとする。また、平文Ｎの暗号化要求があるときは、割り込みＩＴが発生し、平文Ｎの暗号化要求が解除されるまで、割り込みＩＴがオンになり続けるものとする。また、平文Ｍは、鍵K_1を用いて暗号化され、平文Ｎは、鍵K_2を用いて暗号化されるものとする。鍵K_1又は鍵K_2が暗号化モジュール５１に支給されるものとする。

時刻Ｔ０において、鍵K_1が鍵ＫＩとして外部から支給される。セレクタ１５４は、Ａに接続されているので、鍵ＫＩを鍵Ｋとして暗号化モジュール５１に出力する。また、スイッチ１５７がＥに接続されているので、鍵K_1がレジスタ１５６に記憶される。そして、平文ブロックデータM_1の暗号化処理がスタートする。時刻Ｔ０において、平文ブロックデータM_1の暗号化がスタートした場合には、セレクタ５４の入力Ａから一旦イニシャルバリューＩＶが入力された後、セレクタ５４はＢに切り替わる。そして、平文ブロックデータM_1が鍵K_1を用いて暗号化されている途中の時刻Ｘにおいて、平文ブロックデータN_1の暗号化を要求する割り込みＩＴが発生したとする。時刻Ｔ１までに、暗号文ブロックデータC_1はメモリ５５に記憶された状態になる。そして、割り込みＩＴの発生により時刻Ｔ１において、鍵K_2が鍵ＫＩとして外部から暗号化モジュール５１に支給される。セレクタ１５４は、Ａに接続されているので、鍵ＫＩを鍵Ｋとして暗号化モジュール５１に出力する。また、時刻Ｔ１において、セレクタ５４は入力をＡに設定する。また、時刻Ｔ１において、スイッチ５７とスイッチ１５７はＦに接続される。従って、鍵K_2は、レジスタ１５６に記憶されない。時刻Ｔ１以降は、鍵K_2を用いて平文ブロックデータN_1の暗号化が行われ、暗号文ブロッ

クデータD_1が出力される。時刻Yにおいて、平文ブロックデータN_1の暗号化が終了し、割り込みＩＴが解除されたものとする。この割り込みＩＴの解除により時刻Ｔ２において、セレクタ５４の入力はＣに切り替えられ、スイッチ５７はＥに接続される。従って、鍵K_1がレジスタ１５６から鍵ＫＩとしてセレクタ１５４に出力され、セレクタ１５４から鍵K_1が鍵Ｋとして暗号化モジュール５１に支給される。また、セレクタ５４がＣに切り替わったことにより、メモリ５５に記憶されていた暗号文ブロックデータC_1が平文ブロックデータM_2の暗号化のために入力され、鍵K_1を用いた暗号化モジュール５１により平文ブロックデータM_2が暗号化されて、暗号文ブロックデータC_2が出力される。時刻Ｔ３以前においては、セレクタ５４の入力はＢに切り替えられ、平文ブロックデータM_3を暗号化する場合には、フィードバックループのフィードバックライン６５からフィードバックされた暗号文ブロックデータC_2が入力され、鍵K_1を用いた暗号化モジュール５１により平文ブロックデータM_3が暗号化されて、暗号文ブロックデータC_3が出力される。

また、時刻Ｔ３以前においては、セレクタ１５４の入力は、Ａに切り替えられる。

セレクタ１５４のオペレーション処理を説明する。

電源がオンになった場合には、入力をＡに設定する。また、割り込みＩＴの発生が確認された場合でも、入力をＡに設定し続ける。割り込みＩＴの解除があるまでは、セレクタ１５４は、入力がＡに設定されたままで動作する。セレクタ１５４は、割り込みＩＴの解除があったことが検知された場合に、入力をＣに設定する。この入力をＣに設定することにより、メモリ５５に記憶された鍵K_1が鍵Ｋとして暗号化モジュール５１に入力されることになる。このＣからの鍵入力による暗号化がスタ

ートした場合には、セレクタ１５４は、入力をＡに設定する。

このようにして、割り込みＩＴの発生に基づき、セレクタ１５４を切り替えることができる。

次に、スイッチ１５７の割り込み処理のオペレーションを説明する。

電源がオンになった場合、そして、その後の最初の平文Ｍの暗号化処理の場合は、スイッチ１５７はＥに接続され、平文Ｍの鍵K_1がレジスタ１５６に記憶される。そして、時刻Ｘにて、割り込みＩＴが発生した場合には、時刻T_1でスイッチ１５７をＥからＦに接続し、平文Ｎの鍵K_2を無視する。そして、時刻Ｙにて、割り込みＩＴの解除が検出された場合には、時刻Ｔ２にて、スイッチ１５７をＦからＥに接続する。このようにして、スイッチ１５７は、割り込みＩＴの発生から解除までは平文Ｎの鍵K_2を無視する。従って、メモリ１５５のレジスタ１５６には、平文Ｍの鍵K_1が記憶され続けることになる。

図２８は、図２０に示した復号装置に対して鍵K_1を保存して再利用する場合の構成を示している。

図２８は、図２０に対してセレクタ１７４とメモリ１７５を追加したものである。セレクタ１７４とメモリ１７５の動作は、図２６に示したセレクタ１５４とメモリ１５５と同じである。

メモリ５５とメモリ１５５は、割り込みＩＴが発生したときの暗号化装置の状態を記憶するメモリの一例である。このように、メモリ５５とメモリ１５５とが暗号化処理の状態を記憶しておくことにより、あるデータの暗号化の最中に他のデータの暗号化を行った場合でも、再びあるデータの暗号化の処理に復帰することができる。即ち、メモリ５５に記憶されたデータとメモリ１５５に記憶された鍵Ｋとを用いることにより、暗号化が中断されたときと全く同じ状態に暗号化装置を復帰させることができ、中断した暗号化処理を続行させることが可能になる。

なお、メモリ１５５とメモリ１７５は、図６，図８に示すメモリ５５と同じ構成のものでもよい。また、図示していないが、図１６，図１８，図２２，図２４に対して、図２６，図２８に示すような構成を追加して鍵K_1を保存するようにしてもよい。

また、図２６のメモリ５５とメモリ１５５とは、同一の動作をするので、１つのメモリに統合してもよい。また、図２８のメモリ７５とメモリ１７５とは、同一の動作をするので、１つのメモリに統合してもよい。

以上のように、この実施の形態に係る復号装置は、１つ以上のブロックデータC_i（ｉ＝１，２，３，・・・，ｍ）からなる第１の処理データ（暗号文Ｃ）と、１つ以上のブロックデータD_j（ｊ＝１，２，３，・・・，ｎ）からなる第２の処理データ（暗号文Ｄ）との復号処理をする復号装置において、復号処理の状態を記憶するメモリ７５を備え、第１の処理データの全ブロックデータ（C_1～C_m）の復号処理が完了する前に第２の処理データの最初のブロックデータD_1の復号処理を開始するとともに、第２の処理データの最初のブロックデータD_1の復号処理を開始する場合に第１の処理データの復号処理の状態を上記メモリに記憶させ、第１の処理データの復号処理を再開する場合に復号装置の復号処理の状態をメモリ７５に記憶した第１の処理データの復号処理の状態に復帰させてから第１の処理データの復号処理を再開することを特徴とする。

また、上記復号装置は、第２の処理データの全ブロックデータ（D_1～D_n）の復号処理の完了する前に第１の処理データの復号処理を再開するとともに、上記メモリ７４は、第１の処理データの復号処理を再開する場合に第２の処理データの復号処理の状態を記憶し、第２の処理データの復号処理を再開する場合は、復号装置の復号処理の状態をメモリ

に記憶した第２の処理データの復号処理の状態に復帰させてから第２の処理データの復号処理を再開することを特徴とする。

ここで、暗号化処理の状態とは、例えば、

図１のＣＢＣモードでは、暗号化ブロックデータC_i（及び鍵K_1）

図１６のＯＦＢモードでは、モジュール出力データT_i（及び鍵K_1）

図１８のＣＦＢモードでは、暗号化ブロックデータC_i（及び鍵K_1）

のことであり、また、復号処理の状態とは、例えば、

図２０のＣＢＣモードでは、暗号化ブロックデータC_i（及び鍵K_1）

図２２のＯＦＢモードでは、モジュール出力データT_i（及び鍵K_1）

図２４のＣＦＢモードでは、暗号化ブロックデータC_i（及び鍵K_1）

のことである。

前述した説明においては、３つのモードの場合の暗号化装置と復号装置を説明したが、前述した３つのモードは一例であり、これらのモードの改良されたもの、或いは、これらのモードが変形されたものであっても構わない。特に、特徴となる点は、先のブロックデータが暗号化復号されたときに生成されたブロックデータC_i又はM_i又はT_iが次のブロックデータM_{i+1}又はC_{i+1}の暗号化復号処理にフィードバックデータとして用いられる暗号化復号方法において、暗号化復号の状態を記憶するメモリ５５を設け、他のデータの暗号化復号化の処理後にブロックデータC_i又はM_i又はT_iを用いて再び元の状態に復帰可能にできる点である。従って、特に暗号化モード、復号モードは問わない。

なお、割り込みＩＴを用いず、ポーリング方式やトークン取得方式等の他のメカニズムを用いて暗号化要求を受け付け、２以上の暗号化復号処理のインタラクティブな並列処理を行うようにしてもよい。

また、暗号鍵Ｋを用いる暗号化復号処理の場合を示したが、暗号鍵Ｋを用いない暗号化復号処理の場合でもよい。

実施の形態２.

この実施の形態においては、暗号化装置が秘匿処理とデータの完全性保証処理を行う場合について説明する。

データの秘匿処理とは、データを暗号化し、データが盗聴されても、或いは、盗まれても意味が分からなくすることである。また、データの完全性保証とは、データが何者かにより置き換えられていることがないことを保証することをいう。データを伝送する場合には、データの秘匿処理を行った上にデータの完全性を保証して伝送したい場合がある。データの秘匿処理は、データを暗号化することにより行われる。データの完全性保証処理は、データの最後に認証子（ＭＡＣ：Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｃｏｄｅ）を付加し、その認証子を検証することにより改竄を発見することにより行われる。

図２９は、ＯＦＢモードの暗号化部１００により秘匿処理を行い、ＣＢＣモードの認証子生成部２００により認証子（ＭＡＣ）を生成する場合を示している。

図２９は、１つ以上の平文ブロックデータからなる平文を暗号化モジュール５１により暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、平文ブロックデータを暗号化モジュール５１により暗号化したときに暗号化モジュール５１が出力したモジュール出力ブロックデータT_iを暗号化モジュール５１へ暗号化モジュールへフィードバックする第１のフィードバックループ６

５を有し、平文ブロックデータを入力し、第１のフィードバックループ６５によりモジュール出力ブロックデータT_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータC_iを出力する暗号化部１００と、認証子演算途中結果T_iをフィードバックする第２のフィードバックループ６６を有し、暗号化部１００から暗号文ブロックデータC_iが出力されるたびに暗号文ブロックデータC_iを入力し、認証子演算処理を行い、第２のフィードバックループ６６により認証子演算途中結果T_iをフィードバックさせ、暗号文の完全性を保証するための認証子Ｐを生成する認証子生成部２００とを備えたことを特徴とする。

図３０は、図２９に示す暗号化装置の動作手順を示す図である。

平文ブロックデータM_1が、まず暗号文ブロックデータC_1に暗号化される。次に、平文ブロックデータM_2が入力され、暗号文ブロックデータC_2に暗号化される。この平文ブロックデータM_2の暗号化と同じ時刻に暗号文ブロックデータC_1が入力され、認証子の演算が始まる。時刻Ｔ１とＴ２の間に平文ブロックデータM_2の暗号化と暗号文ブロックデータC_1に基づく認証子演算が行われる。また、時刻Ｔ２とＴ３の間では、平文ブロックデータM_3の暗号化と暗号文ブロックデータC_2に基づく認証子の演算が行われる。時刻Ｔ３においては、暗号文ブロックデータC_3に基づく認証子の演算が行われ、認証子Ｐが出力される。

図２９で特徴となる点は、排他的論理和回路５８から出力される暗号文ブロックデータC_iがフィードライン６９により排他的論理和回路５９に入力されている点である。フィードライン６９によりＯＦＢモードとＣＢＣモードの暗号化処理を結合することにより、図３０に示すように、秘匿処理と完全性認証処理がパイプライン処理で実行される。図５２に示した場合は、時刻Ｔ６で処理時間がかかったが、図３０の場合は、時刻Ｔ４で処理が終了して高速処理が行われたことになる。

図３１は、図２９に示した暗号化装置の動作フローチャート図である。

Ｓ５１において、ブロックデータカウンタｉを１とする。Ｓ５２は、暗号化部１００の動作であり、暗号化部１００は、平文ブロックデータM_iを入力して平文ブロックデータM_iを暗号化し、暗号文ブロックデータC_iを生成して暗号文ブロックデータC_iを出力する。Ｓ５３は、認証子生成部２００の動作であり、暗号文ブロックデータC_iを入力し暗号文ブロックデータC_iを暗号化し、認証子を演算する。Ｓ５４は、ブロックデータカウンタｉが最後のブロックデータｎを示しているかどうかを判断し、最後のブロックデータでない場合には、Ｓ５５において、ブロックデータカウンタｉを増加させ、再びＳ５２の処理に戻る。即ち、暗号化部１００と認証子生成部２００の処理を繰り返す。Ｓ５４において、最後のブロックデータの処理が終了した場合には、Ｓ５３で演算された直前の認証子が最終的な認証子であるから、Ｓ５６において、その認証子を暗号文ブロックデータC_iの最後に付加する。図３１に示すように、暗号化部１００が暗号文ブロックデータC_iを生成するたびに、認証子生成部２００が暗号文ブロックデータC_iを入力して認証子を演算することによりパイプライン処理が可能になり、高速処理が行われる。

図３２は、図２９に示した暗号化部１００と認証子生成部２００をあわせたものである。即ち、暗号化部１００と認証子生成部２００の暗号化モジュール５１を兼用し、また、暗号化部１００と認証子生成部２００の排他的論理和回路５８と５９を兼用したものである。更には、暗号化部１００のフィードバックライン６５と認証子生成部２００のフィードバックライン６６を兼用したものである。

第１セレクタ６１は、秘匿処理の開始時にイニシャルバリューＩＶを

選択するものである。第２セレクタ６２は、完全性保証処理の開始時にイニシャルバリューＩＶを選択するものである。第３セレクタ６３は、秘匿処理と完全性保証処理を交互に選択するものである。第３セレクタ６３は入力をＥにすることにより、秘匿処理を行わせることができる。また、第３セレクタ６３は入力をＦにすることにより、完全性保証処理を行わせることができる。

メモリ９３は、暗号鍵Ｋを用いた暗号化モジュール５１から出力されたモジュール出力データT_iを記録するものである。メモリ９３は、入力スイッチ９６と出力スイッチ９７と第１レジスタ９８と第２レジスタ９９により構成されている。入力スイッチ９６と出力スイッチ９７は、第３セレクタ６３の切り替えと同期しており、第３セレクタ６３が切り替わるたびに入力スイッチ９６及び出力スイッチ９７も切り替わる。

図３３は、図３２に示す暗号化装置の動作手順を示す図である。

時刻Ｔ０とＴ１の間で平文ブロックデータM_1の秘匿処理が行われる。秘匿処理の途中で生成されたモジュール出力データは、第１レジスタ９８に記憶される。時刻Ｔ１とＴ２の間では、暗号文ブロックデータC_1に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第２レジスタ９９に記憶される。次に、時刻Ｔ２とＴ３の間では、第１レジスタ９８に記憶されたモジュール出力データと平文ブロックデータM_2に基づいて平文ブロックデータM_2の秘匿処理が行われる。次に、時刻Ｔ３とＴ４の間では、第２レジスタ９９に記憶された認証子中間演算結果と暗号文ブロックデータC_2が入力され、認証子の演算が行われる。この動作を繰り返すことにより、秘匿処理と完全性認証処理が完了し、暗号文と認証子Ｐが出力される。図３３に示す場合は、時刻Ｔ６までで処理が終了し、時間の短縮は図られていないが、図３２に示すように、暗号鍵Ｋを用いた暗号化モジュール５１と

排他的論理和回路５８とフィードバックライン６７，６８（フィードバックループ）が兼用されているので、回路規模を小さくすることができる。

図３４は、ＯＦＢモードの復号化部３００とＣＢＣモードの認証子生成部４００を有する復号装置を示す図である。

この認証子生成部４００は、認証子生成部２００と同一構成のものである。

図３４は、１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、暗号文ブロックデータC_iを復号モジュール７１により復号したときに生成したモジュール出力ブロックデータT_iをフィードバックする第１のフィードバックループ６５を有し、暗号文ブロックデータC_iを入力し、第１のフィードバックループ６５によりモジュール出力ブロックデータT_iをフィードバックさせ復号処理を行い、平文ブロックデータM_iを出力する復号部３００と、認証子演算途中結果T_iをフィードバックする第２のフィードバックループ６６を有し、復号部３００に入力される暗号文ブロックデータC_iと同一の暗号文ブロックデータを入力し、認証子演算処理を行い認証子演算途中結果T_iを出力し、第２のフィードバックループ６６により認証子演算途中結果T_iをフィードバックさせ、暗号文の完全性を確認するための認証子Ｑを生成する認証子生成部４００とを備えたことを特徴とする。

暗号文ブロックデータC_iは、復号化部３００の排他的論理和回路７８に入力されると同時に、フィードライン６９により認証子生成部４００に入力される。このような構成により、復号化部３００と認証子生成部４００の処理が同時並列実行され、処理速度が向上する。

図３５は、図３４に示した復号装置の復号化部３００と認証子生成部

４００を一体化したものである。

図３５は、暗号鍵Ｋを用いた復号モジュール７１とフィードバックライン８７，８８（フィードバックループ）が兼用されている場合を示している。

第１セレクタ８１は、復号処理の開始時にイニシャルバリューＩＶを選択するものである。第２セレクタ８２は、完全性保証処理の開始時にイニシャルバリューＩＶを選択するものである。第３セレクタ８３は、復号処理と完全性保証処理を交互に選択するものである。第３セレクタ８３は入力をＥにすることにより、復号処理を行わせることができる。また、第３セレクタ８３は入力をＦにすることにより、完全性保証処理を行わせることができる。

メモリ９３は、暗号鍵Ｋを用いた暗号化モジュール５１から出力されたモジュール出力データT_iを記録するものである。メモリ９３は、入力スイッチ９６と出力スイッチ９７と第１レジスタ９８と第２レジスタ９９により構成されている。入力スイッチ９６と出力スイッチ９７は、第３セレクタ８３の切り替えと同期しており、第３セレクタ８３が切り替わるたびに入力スイッチ９６及び出力スイッチ９７も切り替わる。

図３６は、図３５に示した復号装置の動作手順を示す図である。

復号装置は、暗号文と認証子Ｐを入力する。

時刻Ｔ０とＴ１の間で暗号文ブロックデータC_1の復号処理と暗号文ブロックデータC_1のレジスタ１１１への保存が行われる。復号処理の途中で生成されたモジュール出力データは、第１レジスタ９８に記憶される。時刻Ｔ１とＴ２の間では、レジスタ１１１に保存された暗号文ブロックデータC_1に基づく認証子の演算が行われる。完全性保証処理により生成された認証子演算途中結果は、第２レジスタ９９に記憶される。次に、時刻Ｔ２とＴ３の間では、暗号文ブロックデータC_2がレジス

タ１１１に保存され、第１レジスタ９８に記憶されたモジュール出力データと暗号文ブロックデータC_2に基づいて平文ブロックデータM_2の復号処理が行われる。次に、時刻Ｔ３とＴ４の間では、第２レジスタ９９に記憶された認証子中間演算結果とレジスタ１１１に保存された暗号文ブロックデータC_2が入力され、認証子の演算が行われる。この動作を繰り返すことにより、平文と認証子Ｑが出力される。この認証子Ｑは、認証子Ｐと比較され、認証子Ｐと認証子Ｑが一致していれば、データの完全性が認証できたことになる。これで、復号処理と完全性認証処理が完了する。

図３７は、図２９のＯＦＢモードの暗号化部１００をＣＢＣモードの暗号化部１００にしたものである。

図３７は、１つ以上の平文ブロックデータからなる平文を暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、平文ブロックデータを暗号化ユニット５２により暗号化したときに暗号化モジュール５１が出力した暗号文ブロックデータC_iをフィードバックする第１のフィードバックループ６５を有し、平文ブロックデータM_iを入力し、第１のフィードバックループ６５により暗号文ブロックデータC_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータC_iを出力する暗号化部１００と、認証子演算途中結果T_iをフィードバックする第２のフィードバックループ６６を有し、暗号化部１００から暗号文ブロックデータC_iが出力されるたびに暗号文ブロックデータC_iを入力し、認証子演算処理を行い、第２のフィードバックループ６６により認証子演算途中結果T_iをフィードバックさせ、暗号文の完全性を保証するための認証子Ｐを生成する認証子生成部４００とを備えたことを特徴とする。

図３８は、図３４のＯＦＢモードの復号部３００をＣＢＣモードの復

号部３００にしたものである。

図３８は、１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、暗号文ブロックデータC_iをフィードバックする第１のフィードバックループ８５，８２を有し、暗号文ブロックデータC_iを入力し、第１のフィードバックループ８５，８２により暗号文ブロックデータC_iをフィードバックさせ復号処理を行い、平文ブロックデータM_iを出力する復号部３００と、認証子演算途中結果T_iをフィードバックする第２のフィードバックループ６６を有し、復号部３００に入力される暗号文ブロックデータC_iと同一の暗号文ブロックデータC_iを入力し、認証子演算処理を行い認証子演算途中結果T_iを出力し、第２のフィードバックループにより認証子演算途中結果T_iをフィードバックさせ、暗号文の完全性を確認するための認証子Ｑを生成する認証子生成部４００とを備えたことを特徴とする。

以上のように、図２９，図３７は、データを入力して暗号化し、暗号データを出力する暗号化部と、暗号化部が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、認証子生成部は、暗号化部によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする暗号化装置を示している。

また、図３４，図３８は、データを入力して復号し、復号データを出力する復号部と、復号部が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部とを備え、認証子生成部は、復号部によるデータの復号が完了する前に認証子の生成を開始することを特徴とする復号装置を示している。

なお、図示していないが、ＯＦＢモードの暗号化部１００又は復号部３００を用いてもよい。

また、図示していないが、ＯＦＢモード又はＣＦＢモードの認証子生成部２００を用いてもよい。

図３９は、暗号化モジュール５１又は復号モジュール７１の構成図である。

暗号化モジュール５１は、鍵スケジュール部５１１とデータランダマイズ部５１２を有している。鍵スケジュール部５１１は、１つの鍵Ｋを入力してｎ個の拡大鍵$ExtK_1$～$ExtK_n$を生成する。データランダマイズ部５１２は、関数ＦとＸＯＲ回路とにより乱数を発生させる。関数Ｆは、拡大鍵を入力して非線形データ変換を行う。

上記暗号化装置の暗号モジュール５１においては、例えば、

（１）ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）、又は、

（２）国際公開番号ＷＯ９７／９７０５（米国特許出願番号０８／８３６４０）に開示されたブロック暗号アルゴリズムであるＭＩＳＴＹ、又は、

（３）上記ブロック暗号アルゴリズムＭＩＳＴＹをベースとした６４ビットブロック暗号であり、次世代携帯電話用国際標準暗号（ＩＭＴ２０００）として採用されることが決定されたブロック暗号アルゴリズムであるＫＡＳＵＭＩ（詳細は、ｈｔｔｐ：／／ｗｗｗ．３ｇｐｐ．ｏｒｇ／Ａｂｏｕｔ＿３ＧＰＰ／３ｇｐｐ．ｈｔｍを参照のこと）、又は、

（４）日本特許出願番号２０００－６４６１４（出願日２０００年３月９日）に記載されたブロック暗号アルゴリズムであるＣａｍｅｌｌｉａ

などのブロック暗号アルゴリズムを用いることができる。また、上記復号装置の復号モジュール７１においても、ＤＥＳ、ＭＩＳＴＹ、ＫＡＳＵＭＩ又はＣａｍｅｌｌｉａなどのブロック暗号アルゴリズムを用いる

ことができる。

図４０は、前述した暗号化装置又は復号装置の実装形式を示す図である。

図４０は、ＦＰＧＡ又はＩＣ又はＬＳＩの中に前述した暗号化装置及び復号装置が実現されている場合を示している。即ち、前述した暗号化装置及び復号装置は、ハードウェアで実現することができる。また、図示していないが、プリントサーキットボードにより実現することも可能である。

図４１は、前述した暗号化装置及び復号装置をソフトウェアで実現する場合を示している。

前述した暗号化装置は、暗号化プログラム４７で実現することができる。暗号化プログラム４７は、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）４２（記録媒体の一例）に記憶されている。暗号化プログラム４７は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）又はフレキシブルディスク又は固定ディスク等の他の記録媒体に記録されていてもよい。また、暗号化プログラム４７は、サーバコンピュータからダウンロードされてもよい。暗号化プログラム４７は、サブルーチンとして機能する。暗号化プログラム４７は、ＲＡＭ４５に記憶されたアプリケーションプログラム４６からサブルーチンコールにより呼び出されて実行される。或いは、暗号化プログラム４７は、割り込み制御部４３で受け付ける割り込みの発生により起動されるようにしても構わない。メモリ５５は、ＲＡＭ４５の一部であっても構わない。アプリケーションプログラム４６、暗号化プログラム４７は、ＣＰＵ４１により実行されるプログラムである。

図４２は、アプリケーションプログラム４６が暗号化プログラム４７を呼び出すメカニズムを示している。

アプリケーションプログラム４６は、鍵Ｋとイニシャルバリュー ＩＶと平文Ｍと暗号文Ｃをパラメータにして暗号化プログラム４７を呼び出す。暗号化プログラム４７は、鍵Ｋとイニシャルバリュー ＩＶと平文Ｍを入力し、暗号文Ｃを返すものである。暗号化プログラム４７と復号プログラムが同一のときは、鍵Ｋとイニシャルバリュー ＩＶと暗号文Ｃと平文Ｍをパラメータにして暗号化プログラム４７を呼び出す。

また、図示しないが、暗号化プログラム４７は、デジタルシグナルプロセッサと、そのデジタルシグナルプロセッサにより読み込まれて実行されるプログラムによって実現しても構わない。即ち、ハードウェアとソフトウェアの組み合わせによって暗号化プログラム４７を実現しても構わない。

図４０，図４１，図４２は、主として、暗号化装置の場合を説明したが、復号装置でも同様の方式で実現できる。

図４０及び図４１に示したような暗号化装置及び復号装置は、電子機器に対してインストールすることができる。例えば、パーソナルコンピュータやファクシミリ装置や携帯電話やビデオカメラやデジタルカメラやテレビカメラ等のあらゆる電子機器にインストールすることができる。特に、この実施の形態における特徴が発揮できるのは、複数のチャネルからのデータを暗号化復号する場合に有効である。或いは、複数のユーザからのデータがアットランダムに到着して復号する場合に、或いは、複数のユーザに対するデータがアットランダムに発生して、それぞれのデータをリアルタイムに暗号化するような場合に有効である。即ち、暗号化復号するデータの数に比べて暗号化復号する装置の数が少ない場合に、前述した実施の形態の暗号化装置、復号装置が非常に有効である。例えば、多くのクライアントコンピュータをサポートしなければならないサーバコンピュータや多くの携帯電話機からのデータを集配しなけ

ればならない基地局や回線コントローラなどに、前述した暗号化装置や復号装置が非常に有効である。

なお、暗号化処理同士及び復号処理同士の並列処理でなく、暗号化処理と復号処理との並列処理を行うようにしてもよい。

また、ＯＦＢモードの暗号化部（又は復号化部）とＣＢＣモードの認証子生成部との組み合わせの場合を示したが、ＯＦＢモードとＣＢＣモードとＣＦＢモードとこれらのモードの改良モードとその他のモードとのいずれのモードの組み合わせでも構わない。

また、認証子生成部が、暗号鍵Ｋを用いた暗号化を行う場合を示したが、認証子生成部は、データの攪拌や演算やその他のデータ処理を行う場合であっても構わない。

産業上の利用可能性

以上のように、この発明の好適な実施の形態によれば、平文Ｍの暗号化の途中で平文Ｎの暗号化を開始することができる。また、暗号文Ｃの復号中に他の暗号文Ｄの復号を開始することができる。

また、この発明の好適な実施の形態によれば、優先度を付けることにより暗号化復号されるデータを優先度に基づいて高速に処理することができる。

また、この発明の好適な実施の形態によれば、秘匿処理と完全性保証処理とを並列処理することにより高速処理が行える。また、秘匿処理と完全性保証処理を統合化された１つのハードウェアで行うことができる。

請求の範囲

1．第１の処理データと、第２の処理データとの暗号化処理をする暗号化装置において、

暗号化処理の状態を記憶するメモリを備え、

第１の処理データの暗号化処理が完了する前に第２の処理データの暗号化処理を開始するとともに、第２の処理データの暗号化処理を開始する場合に第１の処理データの暗号化処理の状態を上記メモリに記憶させ、第１の処理データの暗号化処理を再開する場合に、暗号化装置の暗号化処理の状態を、メモリに記憶した第１の処理データの暗号化処理の状態に復帰させてから第１の処理データの暗号化処理を再開することを特徴とする暗号化装置。

2．上記暗号化装置は、第２の処理データの暗号処理の完了する前に第１の処理データの暗号化処理を再開するとともに、上記メモリは、第１の処理データの暗号化処理を再開する場合に第２の処理データの暗号化処理状態を記憶し、第２の処理データの暗号化処理を再開する場合は、暗号化装置の暗号化処理の状態を、メモリに記憶した第２の処理データの暗号化処理の状態に復帰させてから第２の処理データの暗号化処理を再開することを特徴とする請求項１記載の暗号化装置。

3．上記第１の処理データは、第１の平文であり、上記第２の処理データは、第２の平文であることを特徴とする請求項１記載の暗号化装置。

4．上記暗号化装置は、割り込みにより第２の処理データの暗号化処理を開始することを特徴とする請求項１記載の暗号化装置。

5．平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，

2，3，・・・）とを暗号化する暗号化装置において、

平文Mの暗号化処理中に平文Nの暗号化要求を平文Mの暗号化処理完了前に受け付けるメカニズムと、

平文ブロックデータM_i の暗号化処理を行い暗号文ブロックデータC_i を出力する暗号化ユニットと、

暗号化ユニットから出力された暗号文ブロックデータC_i をフィードバックラインを介し暗号化ユニットにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Nの暗号化要求を受け付け、平文Nのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1} が平文ブロックデータM_i の次に続けて暗号化されない場合、フィードバックされる暗号文ブロックデータC_i を記憶するメモリと、

平文ブロックデータM_{i+1} が平文ブロックデータM_i の次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされる暗号文ブロックデータC_i を選択してフィードバックループに供給し、上記平文ブロックデータM_{i+1} が平文ブロックデータM_i の次に続けて暗号化されず、平文Nのいずれかの平文ブロックデータの次に暗号化される場合は、上記メモリに記憶された暗号文ブロックデータC_i を選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする暗号化装置。

6．上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項5記載の暗号化装置。

7．暗号化モジュールから出力される暗号文ブロックデータC_i（i＝1，2，3，・・・）を用いて第1の平文Mの平文ブロックデータM_i（i＝1，2，3，・・・）を暗号化する工程と、

上記平文ブロックデータM_iを暗号化している途中で又は平文ブロックデータM_iを暗号化した後に、第1の平文Mの平文ブロックデータM_{i+1}の暗号化に用いられる暗号文ブロックデータC_iをメモリに記憶する工程と、

上記平文ブロックデータM_{i+1}の暗号化に用いられる暗号文ブロックデータC_iをメモリに記憶した後に、第2の平文Nの少なくとも1つの平文ブロックデータを暗号化する工程と、

上記第2の平文Nの少なくとも1つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータM_{i+1}の暗号化に用いられる暗号文ブロックデータC_iを入力し、暗号化モジュールを用いて第1の平文Mの平文ブロックデータM_{i+1}を暗号化する工程と

を備えたことを特徴とする暗号化方法。

8．1つ以上の平文ブロックデータからなる平文を暗号化ユニット暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータC_iを暗号化ユニットへフィードバックする第1のフィードバックループを有し、平文ブロックデータを入力し、第1のフィードバックループにより暗号文ブロックデータC_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第2のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号

文ブロックデータを入力し、データ処理を行い、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備えたことを特徴とする暗号化装置。

９．上記暗号化部と認証子生成部とは、１つの暗号化モジュールと、１つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする請求項８記載の暗号化装置。

１０．１つ以上の平文ブロックデータからなる平文を暗号化ユニットにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化ユニットにより暗号化したときに暗号化ユニットが出力した暗号文ブロックデータC_iを暗号化ユニットへフィードバックする第１のフィードバック工程を有し、平文ブロックデータを入力し、第１のフィードバックループにより暗号文ブロックデータC_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバック

工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と
を備えたことを特徴とする暗号化方法。

１１．第１の処理データと、第２の処理データとの復号処理をする復号装置において、

復号処理の状態を記憶するメモリを備え、

第１の処理データの復号処理が完了する前に第２の処理データの復号処理を開始するとともに、第２の処理データの復号処理を開始する場合に第１の処理データの復号処理の状態を上記メモリに記憶させ、第１の処理データの復号処理を再開する場合に、復号装置の復号処理の状態を、メモリに記憶した第１の処理データの復号処理の状態に復帰させてから第１の処理データの復号処理を再開することを特徴とする復号装置。

１２．上記復号装置は、第２の処理データの復号処理の完了する前に第１の処理データの復号処理を再開するとともに、上記メモリは、第１の処理データの復号処理を再開する場合に第２の処理データの復号処理状態を記憶し、第２の処理データの復号処理を再開する場合は、復号装置の復号処理の状態を、メモリに記憶した第２の処理データの復号処理の状態に復帰させてから第２の処理データの復号処理を再開することを特徴とする請求項１１記載の復号装置。

１３．上記第１の処理データは、第１の暗号文であり、上記第２の処理データは、第２の暗号文であることを特徴とする請求項１１記載の復号装置。

１４．上記復号装置は、割り込みにより第２の処理データの最初のブロックデータの復号処理を開始することを特徴とする請求項１１記載の復号装置。

１５．暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１

，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータD_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、

暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付けるメカニズムと、

暗号文ブロックデータC_iの復号処理を行い平文ブロックデータM_iを出力する復号ユニットと、

暗号文ブロックデータC_{i+1}を復号するための暗号文ブロックデータC_iをフィードバックラインを介し復号ユニットにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Ｄの復号要求を受け付け、暗号文Ｄのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フィードバックされる暗号文ブロックデータC_iを記憶するメモリと、

暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされる暗号文ブロックデータC_iを選択してフィードバックループに供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Ｄのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶された暗号文ブロックデータC_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする復号装置。

１６．上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項１５記載の復号装置。

１７．復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）を復号する工程と、

上記暗号文ブロックデータC_iを復号している途中で又は暗号文ブロックデータC_iを復号した後に、第１の暗号文Ｃの暗号文ブロックデータC_{i+1}の復号に用いられる暗号文ブロックデータC_iをメモリに記憶する工程と、

上記暗号文ブロックデータC_{i+1}の復号に用いられる暗号文ブロックデータC_iをメモリに記憶した後に、第２の暗号文Ｄの少なくとも１つの暗号文ブロックデータを復号する工程と、

上記第２の暗号文Ｄの少なくとも１つの暗号文ブロックデータを復号した後に、メモリに記憶された、暗号文ブロックデータC_{i+1}の復号に用いられる暗号文ブロックデータC_iを入力し、復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_{i+1}を復号する工程と

を備えたことを特徴とする復号方法。

１８．１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータT_iを復号モジュールへフィードバックする第１のフィードバックループを有し、暗号文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブ

ロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

を備えたことを特徴とする復号装置。

１９．上記復号部と認証子生成部とは、１つの復号モジュールと、１つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと

を備えたことを特徴とする請求項１８記載の復号装置。

２０．１つ以上の暗号文ブロックデータからなる暗号文を平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

復号モジュールによりデータを復号したときに生成したモジュール出力ブロックデータT_iを復号モジュールへフィードバックする第１のフィードバック工程を有し、暗号文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブ

ロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

を備えたことを特徴とする復号方法。

２１．平文Ｍを構成する平文ブロックデータM_i（ｉ＝１，２，３，・・・）と平文Ｎを構成する平文ブロックデータN_j（ｊ＝１，２，３，・・・）とを暗号化する暗号化装置において、

平文Ｍの暗号化処理中に平文Ｎの暗号化要求を平文Ｍの暗号化処理完了前に受け付けるメカニズムと、

暗号化処理を行ったデータをモジュール出力ブロックデータT_iとして出力する暗号化モジュールと、

暗号化モジュールから出力されたモジュール出力ブロックデータT_iをフィードバックラインを介し暗号化モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記平文Ｎの暗号化要求を受け付け、平文Ｎのいずれかの平文ブロックデータの暗号化処理を開始することにより、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されない場合、フィードバックされるモジュール出力ブロックデータT_iを記憶するメモリと、

平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるモジュール出力ブロックデータT_iを選択してフィードバックループに供給し、上記平文ブロックデータM_{i+1}が平文ブロックデータM_iの次に続けて暗号化されず、平文Ｎのいずれか

の平文ブロックデータの次に暗号化される場合は、上記メモリに記憶されたモジュール出力ブロックデータT_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする暗号化装置。

２２．上記メモリは、

複数の平文に対応した複数のレジスタと、

暗号化処理をする平文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項２１記載の暗号化装置。

２３．暗号化モジュールから出力されるモジュール出力ブロックデータT_i（i＝１，２，３，・・・）を用いて第１の平文Mの平文ブロックデータM_i（i＝１，２，３，・・・）を暗号化する工程と、

上記平文ブロックデータM_iを暗号化している途中で又は平文ブロックデータM_iを暗号化した後に、第１の平文Mの平文ブロックデータM_{i+1}の暗号化に用いられるモジュール出力ブロックデータT_iをメモリに記憶する工程と、

上記平文ブロックデータM_{i+1}の暗号化に用いられるモジュール出力ブロックデータT_iをメモリに記憶した後に、第２の平文Nの少なくとも１つの平文ブロックデータを暗号化する工程と、

上記第２の平文Nの少なくとも１つの平文ブロックデータを暗号化した後に、メモリに記憶された、平文ブロックデータM_{i+1}の暗号化に用いられるモジュール出力ブロックデータT_iを入力し、暗号化モジュールを用いて第１の平文Mの平文ブロックデータM_{i+1}を暗号化する工程と

を備えたことを特徴とする暗号化方法。

２４．１つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証する

ための認証子を生成する暗号化装置において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータT_iを暗号化モジュールへフィードバックする第１のフィードバックループを有し、平文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、暗号化部から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備えたことを特徴とする暗号化装置。

２５．上記暗号化部と認証子生成部とは、１つの暗号化モジュールと、１つのフィードバックループとを兼用して暗号化処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

暗号化処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

暗号化処理と認証生成処理とを交互に実行するために、メモリから暗号化処理と認証子生成処理との結果を交互に選択して暗号化モジュールに出力するセレクタと

を備えたことを特徴とする請求項２４記載の暗号化装置。

２６．１つ以上の平文ブロックデータからなる平文を暗号化モジュールにより暗号文にし、暗号文に対して暗号文の完全性を保証するための認証子を生成する暗号化方法において、

平文ブロックデータを暗号化モジュールにより暗号化したときに暗号化モジュールが出力したモジュール出力ブロックデータT_iを暗号化モジュールへフィードバックする第１のフィードバック工程を有し、平文ブロックデータを入力し、第１のフィードバックループによりモジュール出力ブロックデータT_iをフィードバックさせ暗号化処理を行い、暗号文ブロックデータを出力する暗号化工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、暗号化工程から暗号文ブロックデータが出力されるたびに暗号文ブロックデータを入力し、データ処理を行い、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備えたことを特徴とする暗号化方法。

２７．暗号文Ｃを構成する暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）と暗号文Ｄを構成する暗号文ブロックデータD_j（ｊ＝１，２，３，・・・）とを復号する復号装置において、

暗号文Ｃの復号処理中に暗号文Ｄの復号要求を任意の時点で受け付けるメカニズムと、

復号処理を行ったデータをモジュール出力ブロックデータT_iとして出力する復号モジュールと、

復号モジュールから出力されたモジュール出力ブロックデータT_iをフィードバックラインを介し復号モジュールにフィードバックするフィードバックループと、

フィードバックループのフィードバックラインと並列に設けられ、上記暗号文Ｄの復号要求を受け付け、暗号文Ｄのいずれかの暗号文ブロックデータの復号処理を開始することにより、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されない場合、フ

ィードバックされるモジュール出力ブロックデータT_iを記憶するメモリと、

暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号される場合は、上記フィードバックループのフィードバックラインによりフィードバックされるモジュール出力ブロックデータT_iを選択してフィードバックループに供給し、上記暗号文ブロックデータC_{i+1}が暗号文ブロックデータC_iの次に続けて復号されず、暗号文Dのいずれかの暗号文ブロックデータの次に復号される場合は、上記メモリに記憶されたモジュール出力ブロックデータT_iを選択してフィードバックループに供給するセレクタと

を備えたことを特徴とする復号装置。

２８．上記メモリは、

複数の暗号文に対応した複数のレジスタと、

復号処理をする暗号文に対応してレジスタを切り替えるスイッチと

を備えたことを特徴とする請求項２７記載の復号装置。

２９．復号モジュールから出力されるモジュール出力ブロックデータT_i（ｉ＝１，２，３，・・・）を用いて第１の暗号文Ｃの暗号文ブロックデータC_i（ｉ＝１，２，３，・・・）を復号する工程と、

上記暗号文ブロックデータC_iを復号している途中で又は暗号文ブロックデータC_iを復号した後に、第１の暗号文Ｃの暗号文ブロックデータC_{i+1}の復号に用いられるモジュール出力ブロックデータT_iをメモリに記憶する工程と、

上記暗号文ブロックデータC_{i+1}の復号に用いられるモジュール出力ブロックデータT_iをメモリに記憶した後に、第２の暗号文Ｄの少なくとも１つの暗号文ブロックデータを復号する工程と、

上記第２の暗号文Ｄの少なくとも１つの暗号文ブロックデータを復号

した後に、メモリに記憶された、暗号文ブロックデータC_{i+1}の復号に用いられるモジュール出力ブロックデータT_iを入力し、復号モジュールを用いて第１の暗号文Ｃの暗号文ブロックデータC_{i+1}を復号する工程と

を備えたことを特徴とする復号方法。

３０．１つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号装置において、

暗号文ブロックデータC_iを復号ユニットへフィードバックする第１のフィードバックループを有し、暗号文ブロックデータを入力し、第１のフィードバックループにより暗号文ブロックデータC_iをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号部と、

認証子演算途中結果をフィードバックする第２のフィードバックループを有し、復号部に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバックループにより認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成部と

を備えたことを特徴とする復号装置。

３１．上記復号部と認証子生成部とは、１つの復号モジュールと、１つのフィードバックループとを兼用して復号処理と認証子生成処理とを交互に行うとともに、

上記１つのフィードバックループは、

復号処理と認証子生成処理との結果をそれぞれ記録し出力するメモリと、

復号処理と認証生成処理とを交互に実行するために、メモリから復号

処理と認証子生成処理との結果を交互に選択して復号モジュールに出力するセレクタと

を備えたことを特徴とする請求項３０記載の復号装置。

３２．１つ以上の暗号文ブロックデータからなる暗号文を復号ユニットにより平文に復号し、かつ、暗号文に対して暗号文の完全性を確認するための認証子を生成する復号方法において、

暗号文ブロックデータC_iを復号ユニットへフィードバックする第１のフィードバック工程を有し、暗号文ブロックデータを入力し、第１のフィードバックループにより暗号文ブロックデータC_iをフィードバックさせ復号処理を行い、平文ブロックデータを出力する復号工程と、

認証子演算途中結果をフィードバックする第２のフィードバック工程を有し、復号工程に入力される暗号文ブロックデータと同一の暗号文ブロックデータを入力し、データ処理を行い認証子演算途中結果を出力し、第２のフィードバック工程により認証子演算途中結果をフィードバックさせ、暗号文の完全性を確認するための認証子を生成する認証子生成工程と

を備えたことを特徴とする復号方法。

３３．上記請求項７記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

３４．上記請求項１０記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

３５．上記請求項１７記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

３６．上記請求項２０記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

３７．上記請求項２３記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

３８．上記請求項２６記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

３９．上記請求項２９記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

４０．上記請求項３２記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

４１．上記暗号化処理は、ブロック暗号アルゴリズムを用いることを特徴とする請求項１記載の暗号化装置。

４２．上記復号処理は、ブロック暗号アルゴリズムを用いることを特徴とする請求項１１記載の復号装置。

４３．上記メモリは、暗号化処理の状態として、

第１の処理データの暗号化途中結果と、

第１の処理データを暗号化するために用いる暗号鍵と

を記憶することを特徴とする請求項１記載の暗号化装置。

４４．上記メモリは、復号処理の状態として、

第２の処理データの復号途中結果と、

第２の処理データを復号するために用いる復号鍵と

を記憶することを特徴とする請求項１１記載の復号装置。

４５．データを入力して暗号化し、暗号データを出力する暗号化部と、

暗号化部が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備え、

認証子生成部は、暗号化部によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする暗号化装置。

４６．データを入力して復号し、復号データを出力する復号部と、

復号部が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成部と

を備え、

認証子生成部は、復号部によるデータの復号が完了する前に認証子の生成を開始することを特徴とする復号装置。

４７．データを入力して暗号化し、暗号データを出力する暗号化工程と、

暗号化工程が出力した暗号データを入力して暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備え、

認証子生成工程は、暗号化工程によるデータの暗号化が完了する前に認証子の生成を開始することを特徴とする暗号化方法。

４８．データを入力して復号し、復号データを出力する復号工程と、

復号工程が入力したデータを入力して暗号文の完全性を保証するための認証子を生成する認証子生成工程と

を備え、

認証子生成工程は、復号工程によるデータの復号が完了する前に認証子の生成を開始することを特徴とする復号方法。

４９．上記請求項４７記載の暗号化方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

５０．上記請求項４８記載の復号方法の各工程をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

図 1

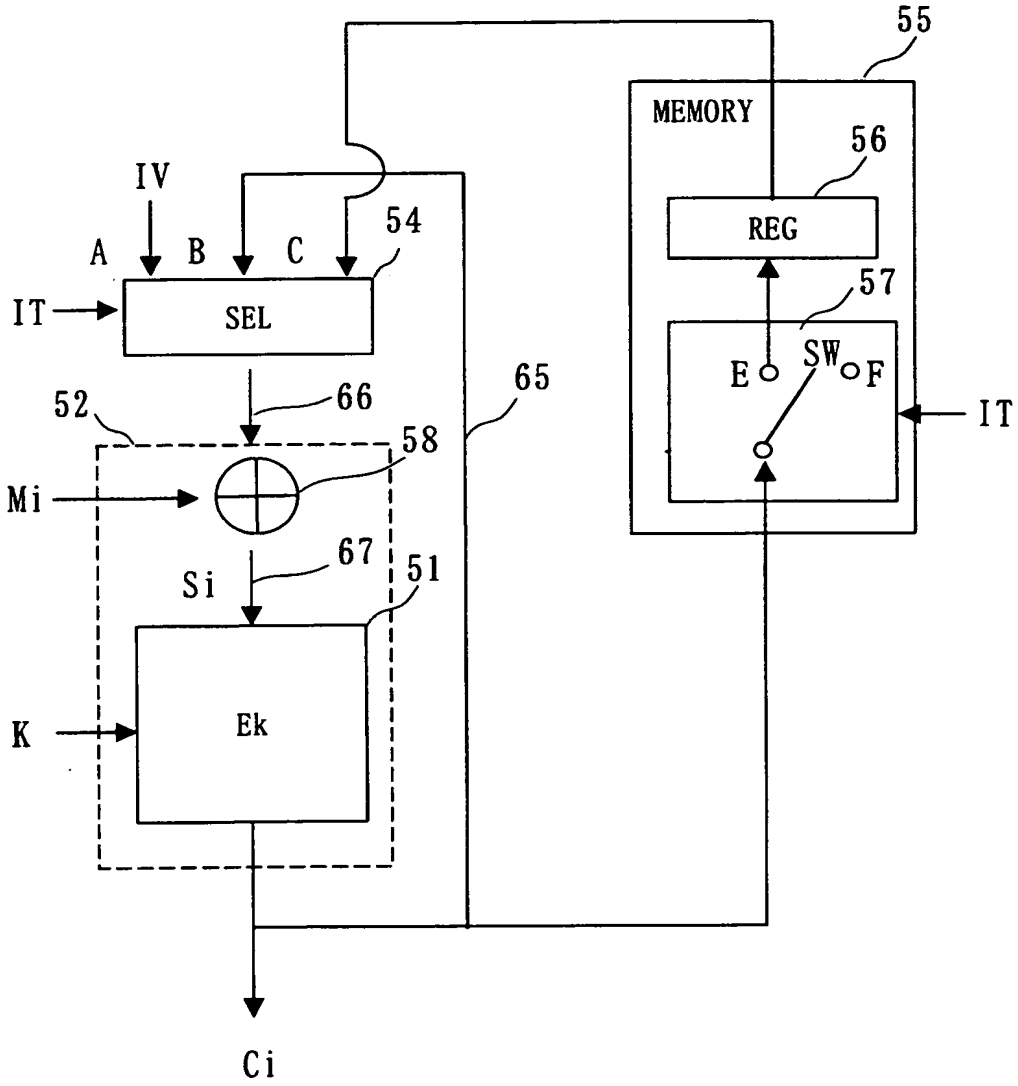

55
MEMORY
56
REG
57
E
SW
F
IT
IV
A
B
C
54
IT
SEL
65
52
66
58
Mi
67
Si
51
K
Ek
Ci

図 2

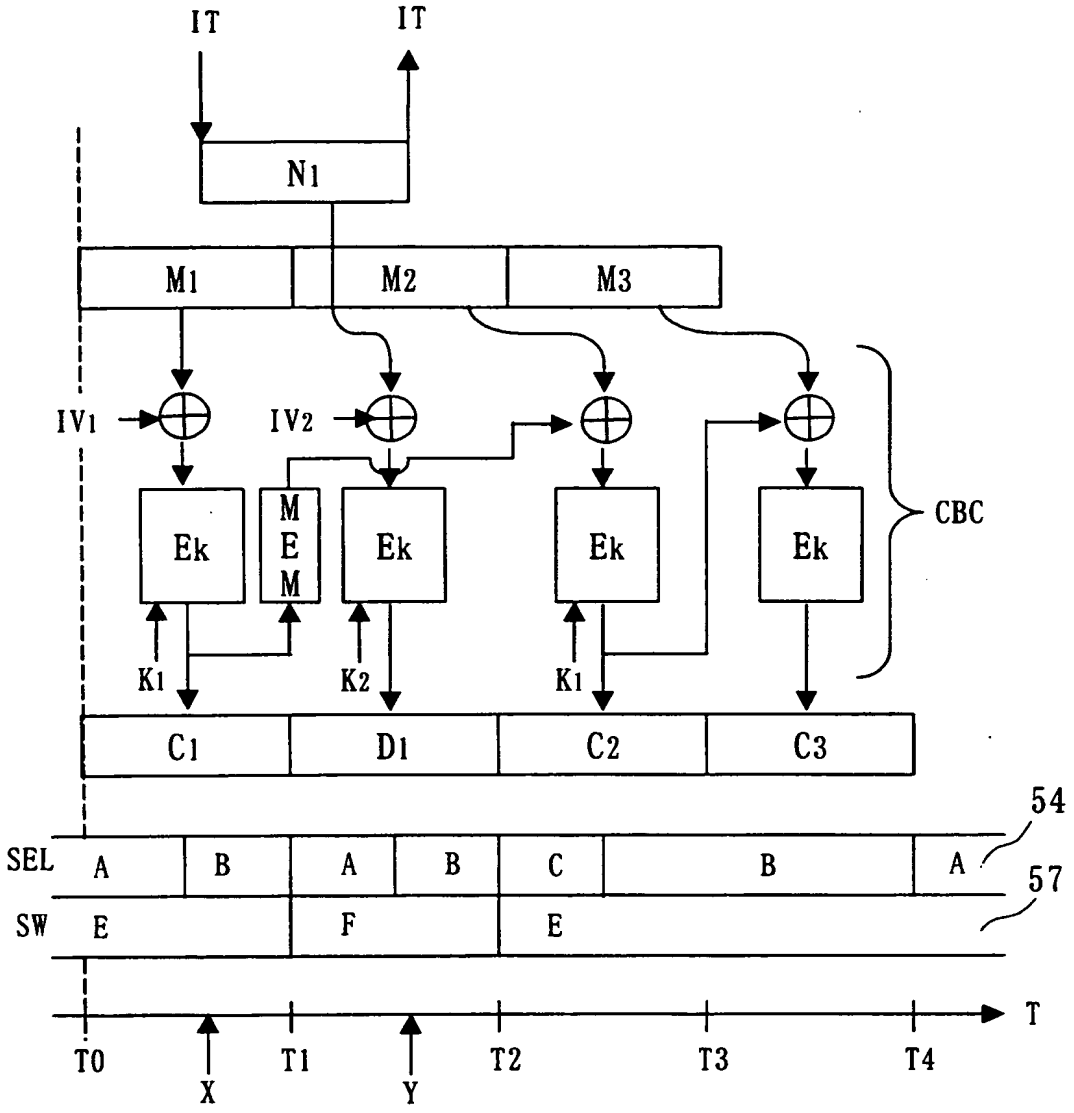

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CBC
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

図 3

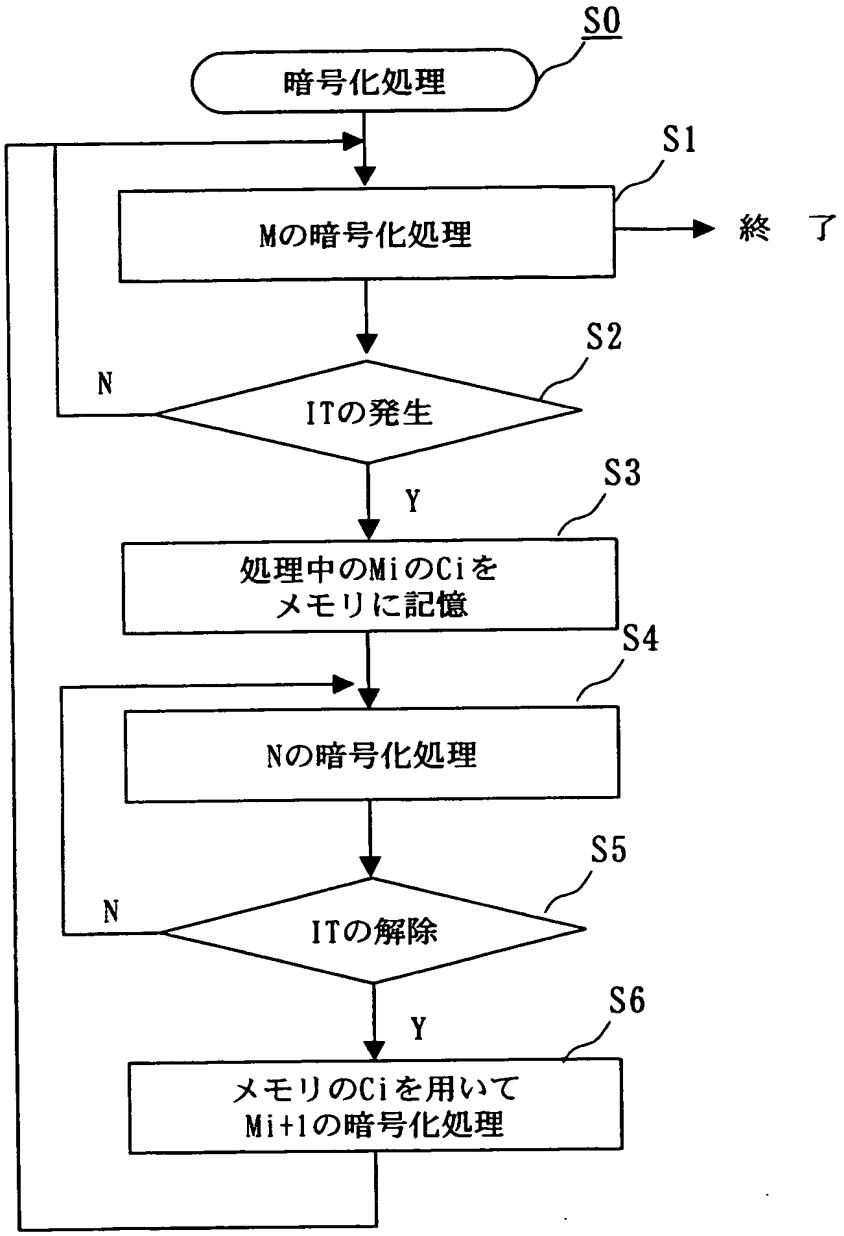

S0
暗号化処理
S1
Mの暗号化処理
終 了
S2
N
ITの発生
Y
S3
処理中のMiのCiを
メモリに記憶
S4
Nの暗号化処理
S5
N
ITの解除
Y
S6
メモリのCiを用いて
Mi+1の暗号化処理

図 4

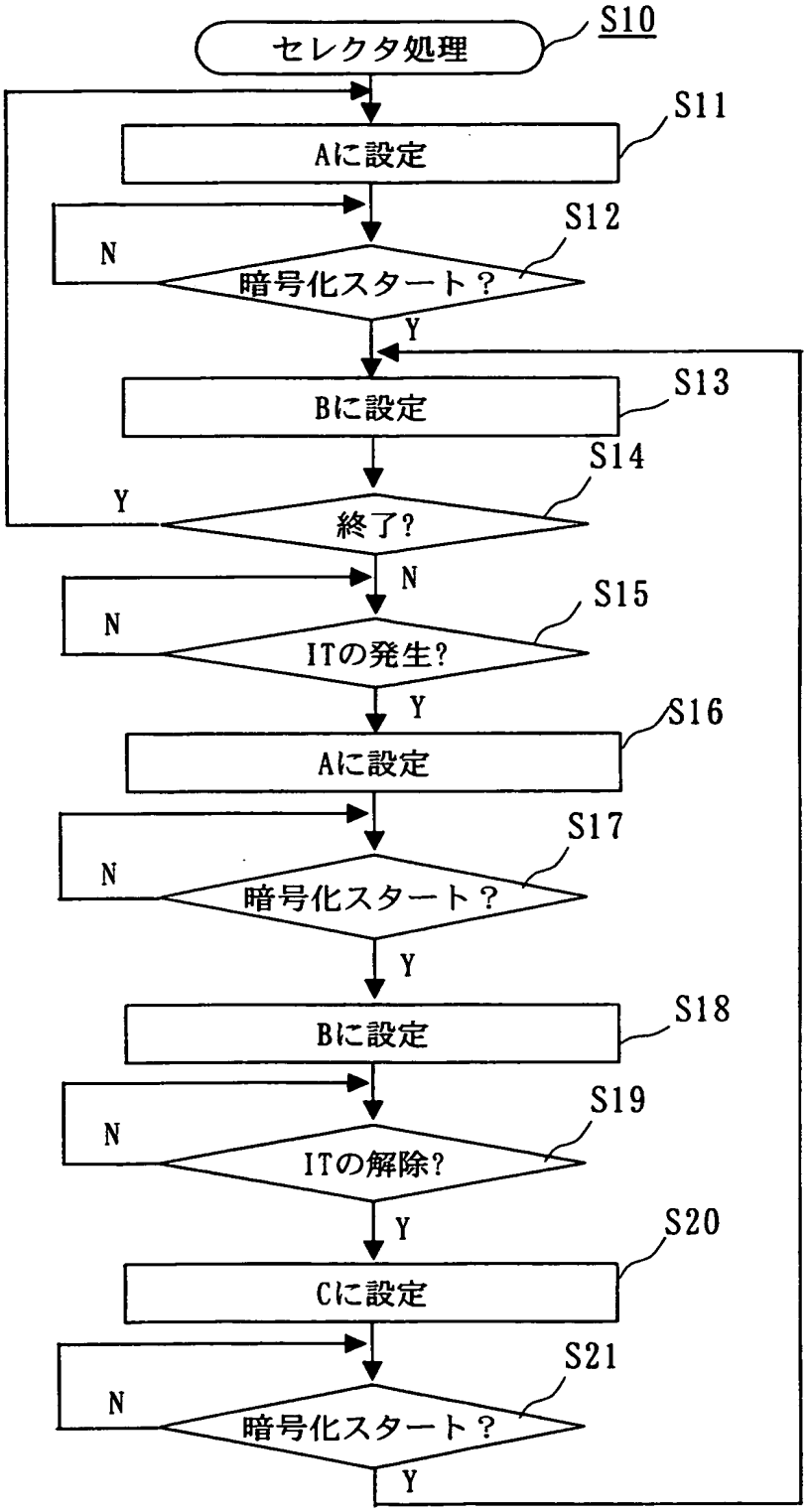

セレクタ処理
S10
Aに設定
S11
暗号化スタート？
S12
N
Y
Bに設定
S13
終了?
S14
Y
N
ITの発生?
S15
N
Y
Aに設定
S16
暗号化スタート？
S17
N
Y
Bに設定
S18
ITの解除?
S19
N
Y
Cに設定
S20
暗号化スタート？
S21
N
Y

図 5

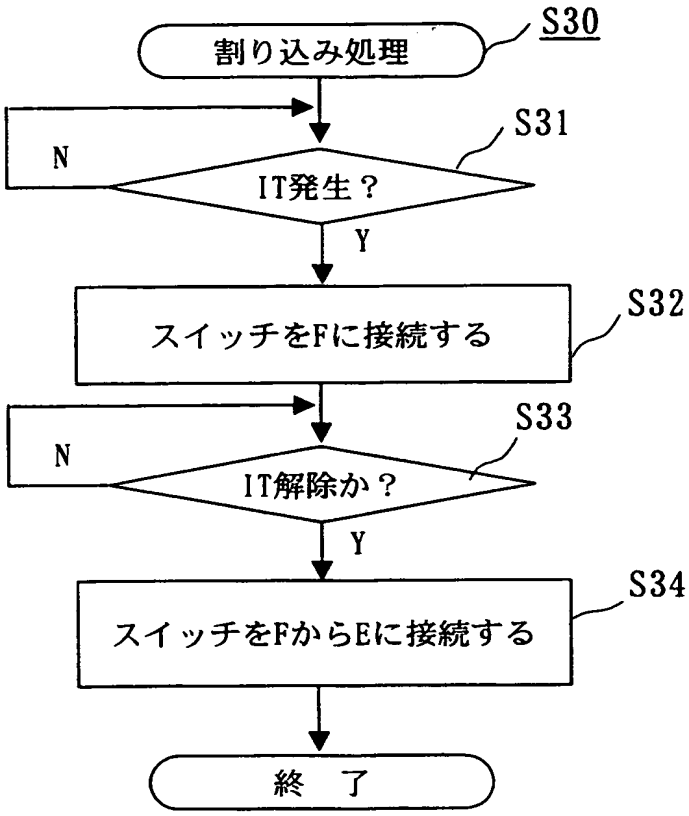

S30
割り込み処理
S31
N
IT発生？
Y
S32
スイッチをFに接続する
S33
N
IT解除か？
Y
S34
スイッチをFからEに接続する
終　了

図 6

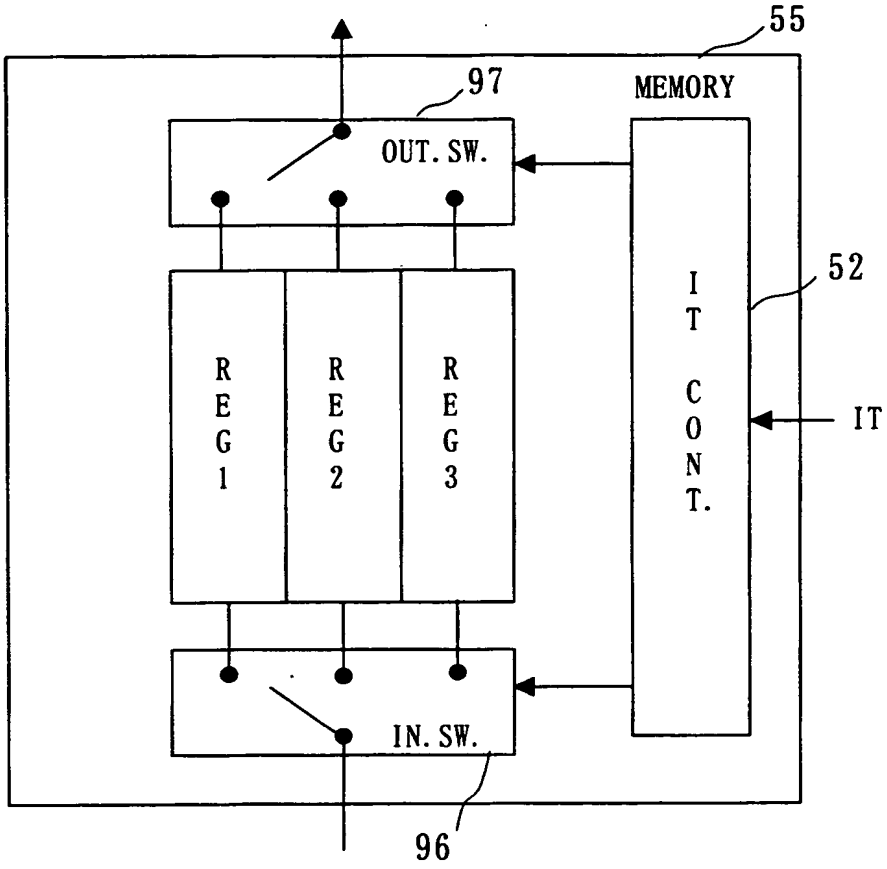


図 7

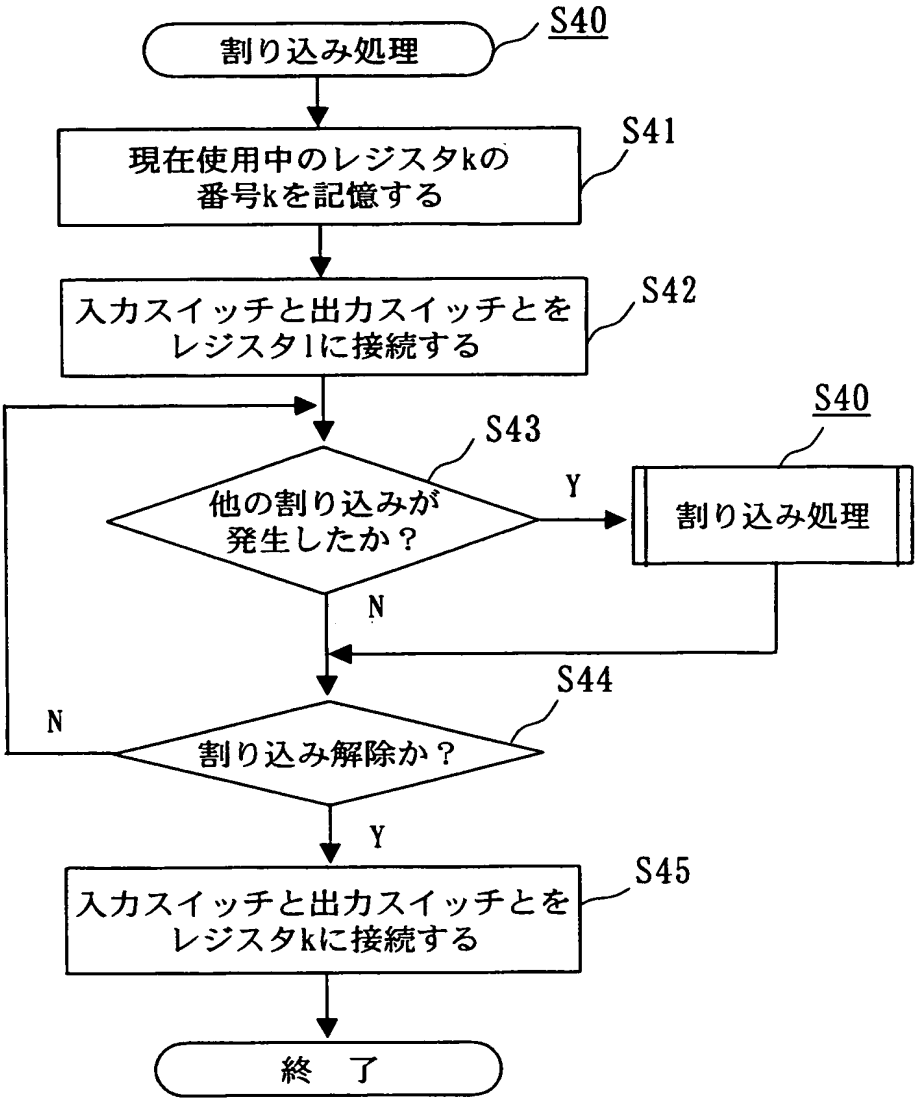

割り込み処理
S40
現在使用中のレジスタkの
番号kを記憶する
S41
入力スイッチと出力スイッチとを
レジスタlに接続する
S42
S40
S43
他の割り込みが
発生したか？
Y
割り込み処理
N
S44
N
割り込み解除か？
Y
入力スイッチと出力スイッチとを
レジスタkに接続する
S45
終　了

図 8

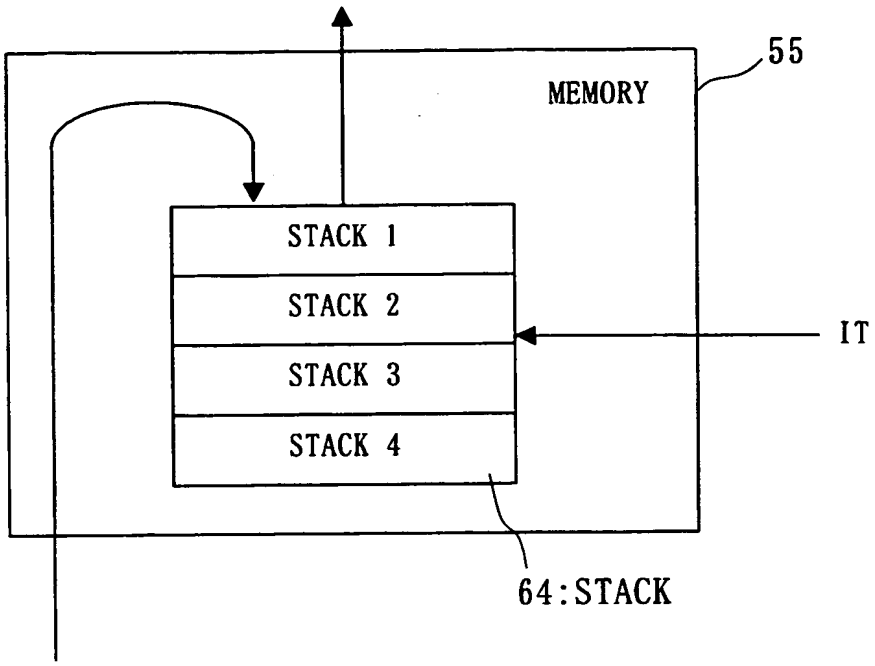

55
MEMORY
STACK 1
STACK 2
STACK 3
STACK 4
IT
64:STACK

図 9

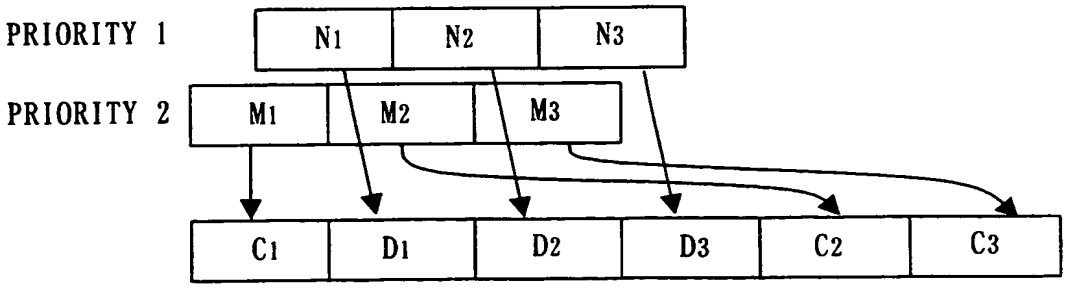

PRIORITY 1
PRIORITY 2
N1
N2
N3
M1
M2
M3
C1
D1
D2
D3
C2
C3

図10

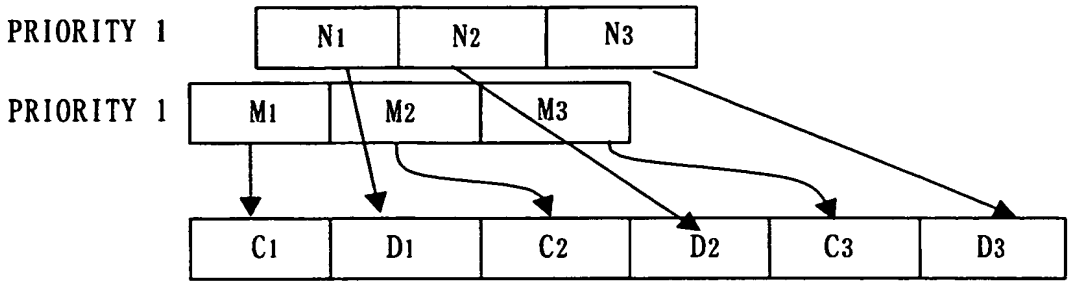

PRIORITY 1
PRIORITY 1
N1
N2
N3
M1
M2
M3
C1
D1
C2
D2
C3
D3

図11

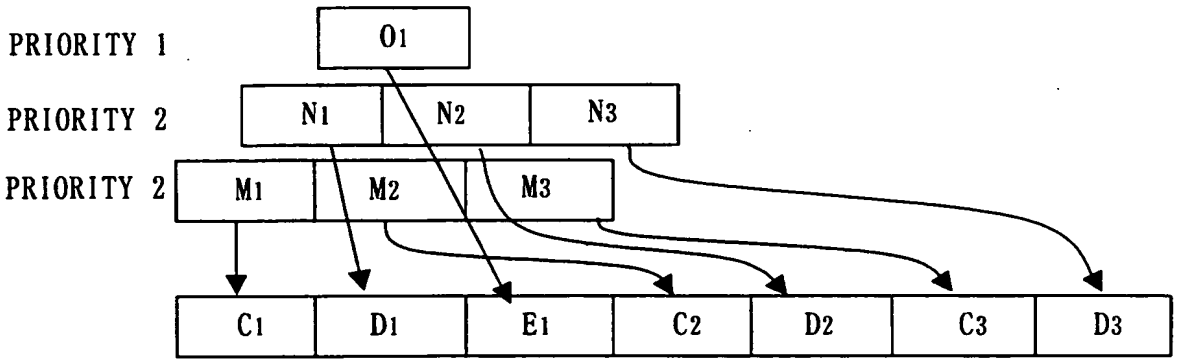

PRIORITY 1
PRIORITY 2
PRIORITY 2
O1
N1
N2
N3
M1
M2
M3
C1
D1
E1
C2
D2
C3
D3

図12

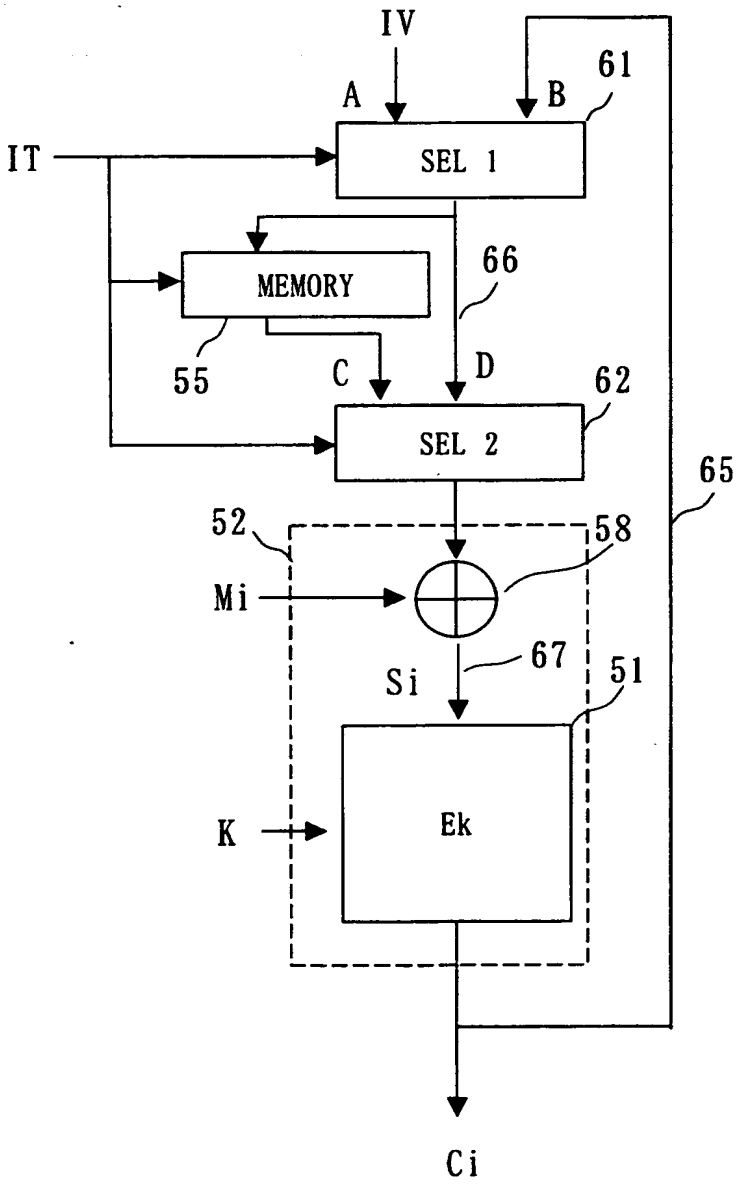


図13

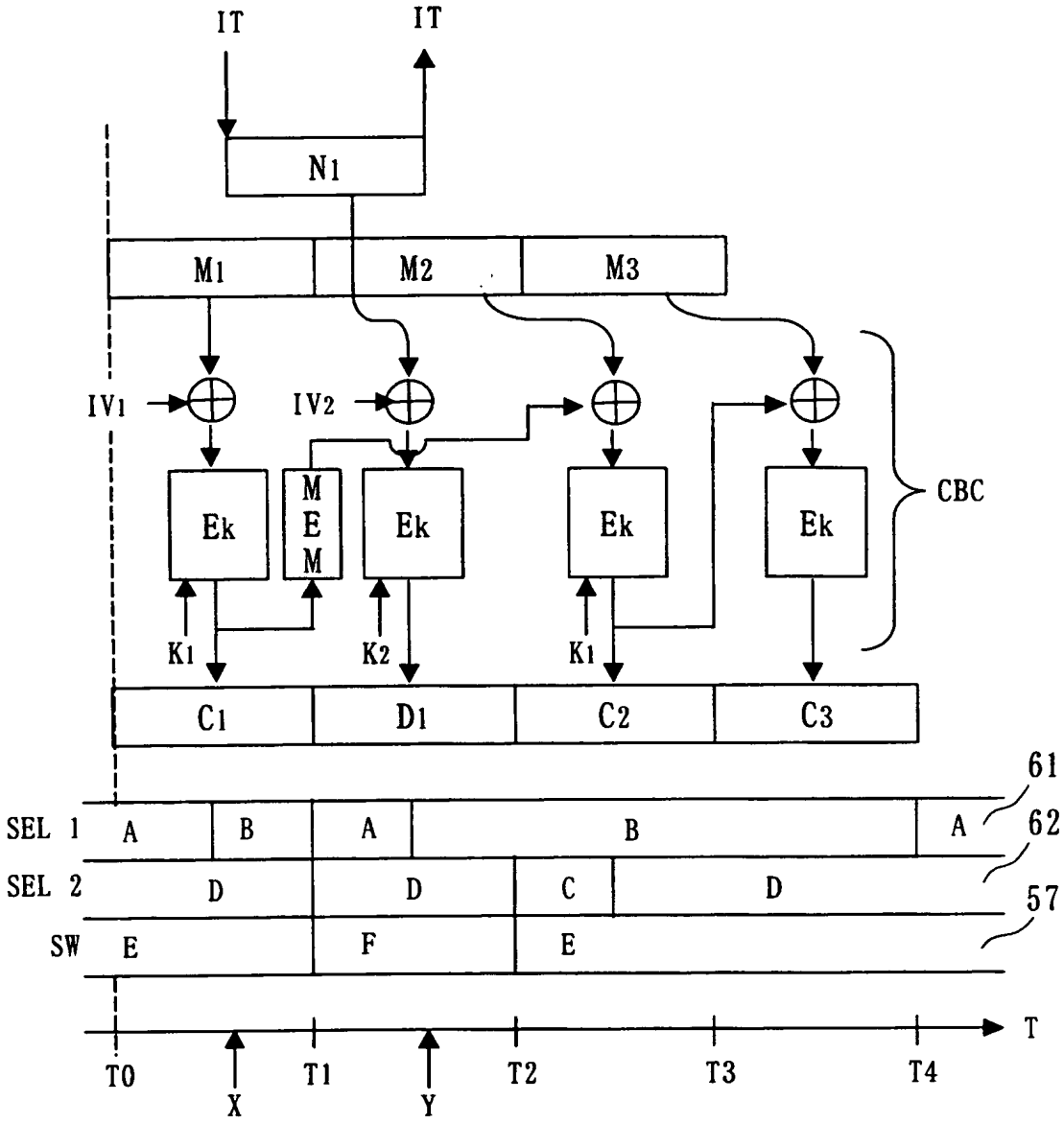

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CBC
K1
K2
K1
C1
D1
C2
C3
61
SEL 1
A
B
A
B
A
62
SEL 2
D
D
C
D
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

図14

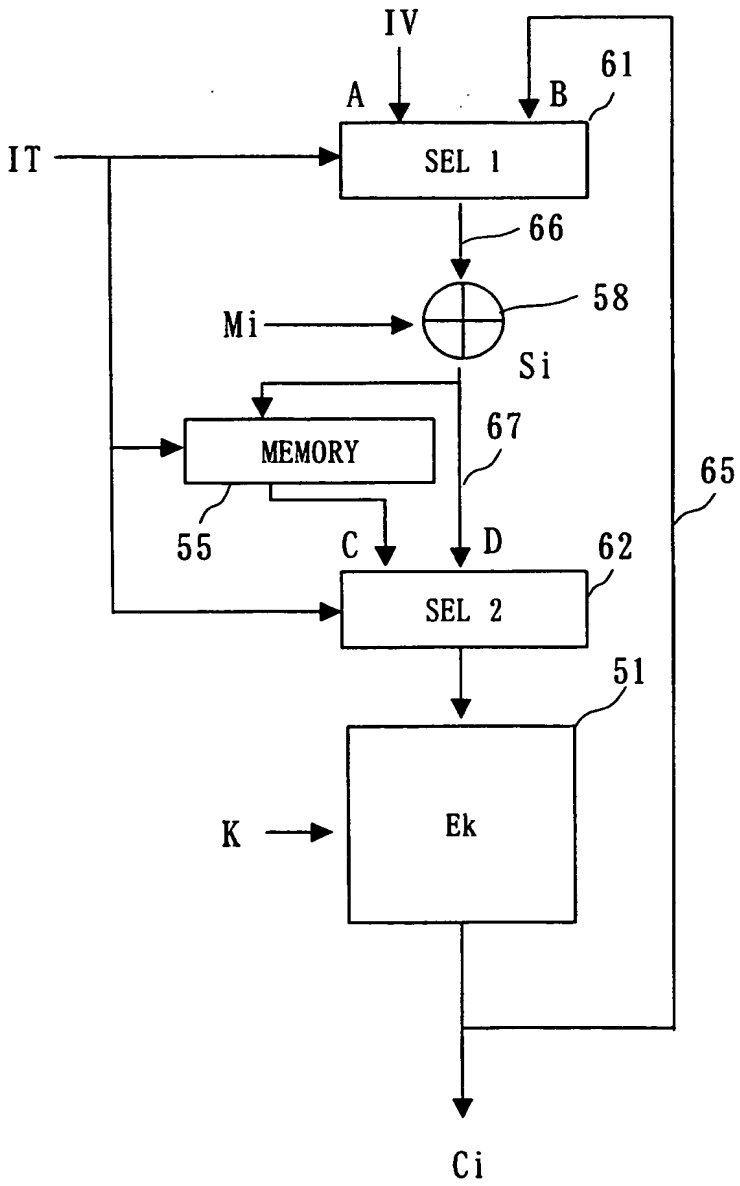


図15

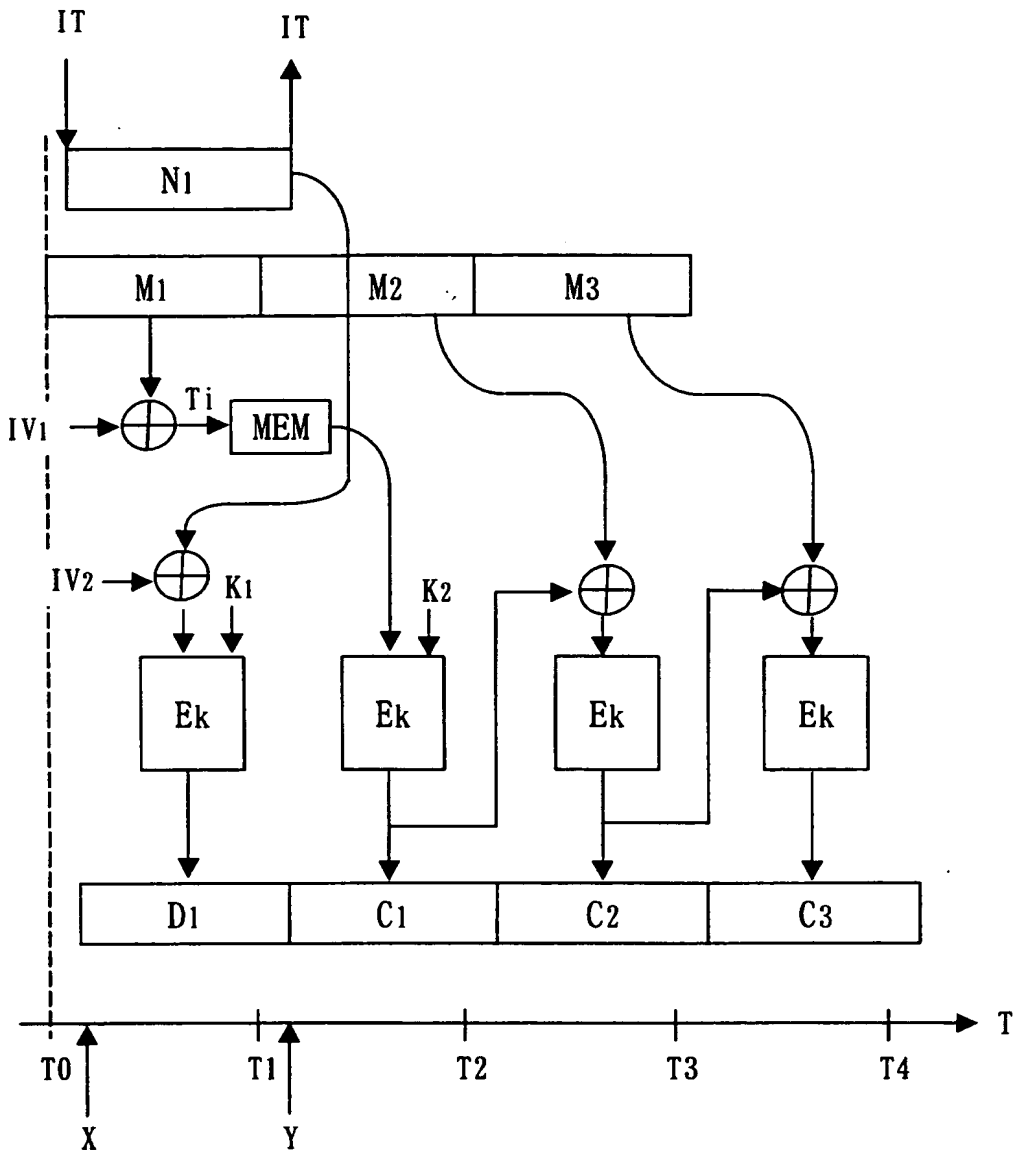

IT
IT
N1
M1
M2
M3
Ti
IV1
MEM
IV2
K1
K2
Ek
Ek
Ek
Ek
D1
C1
C2
C3
T
T0
T1
T2
T3
T4
X
Y

図16

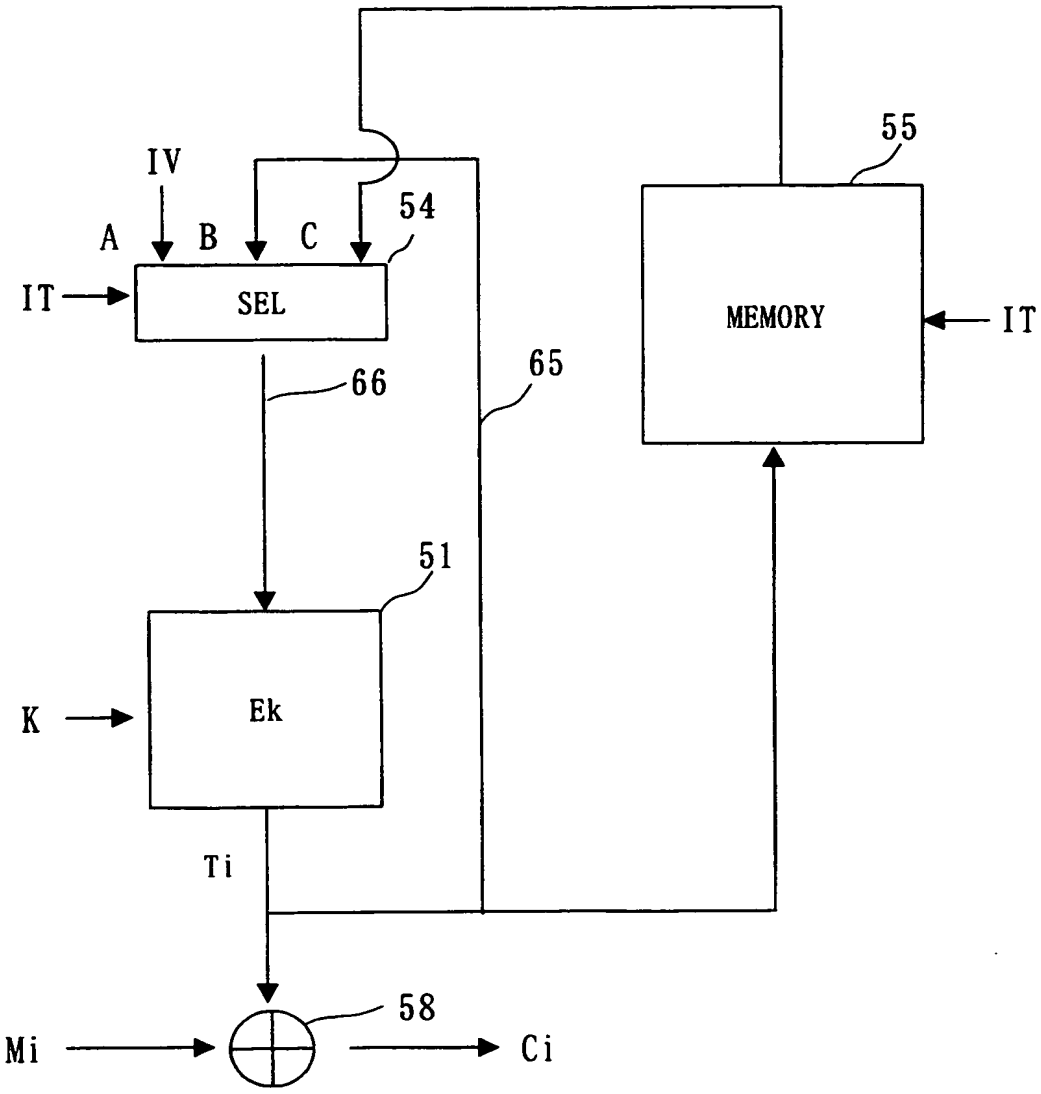


図17

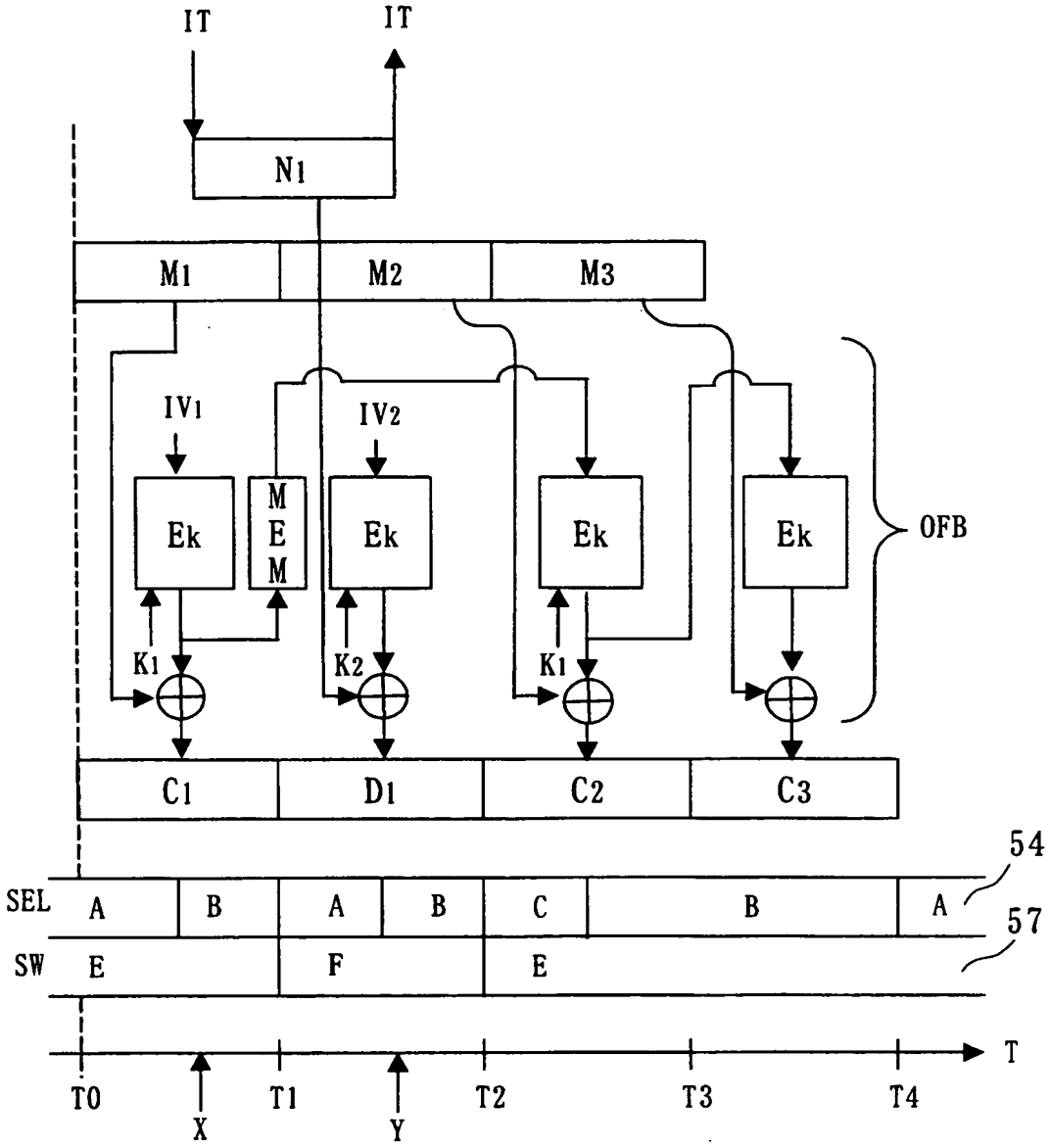

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
OFB
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

図18

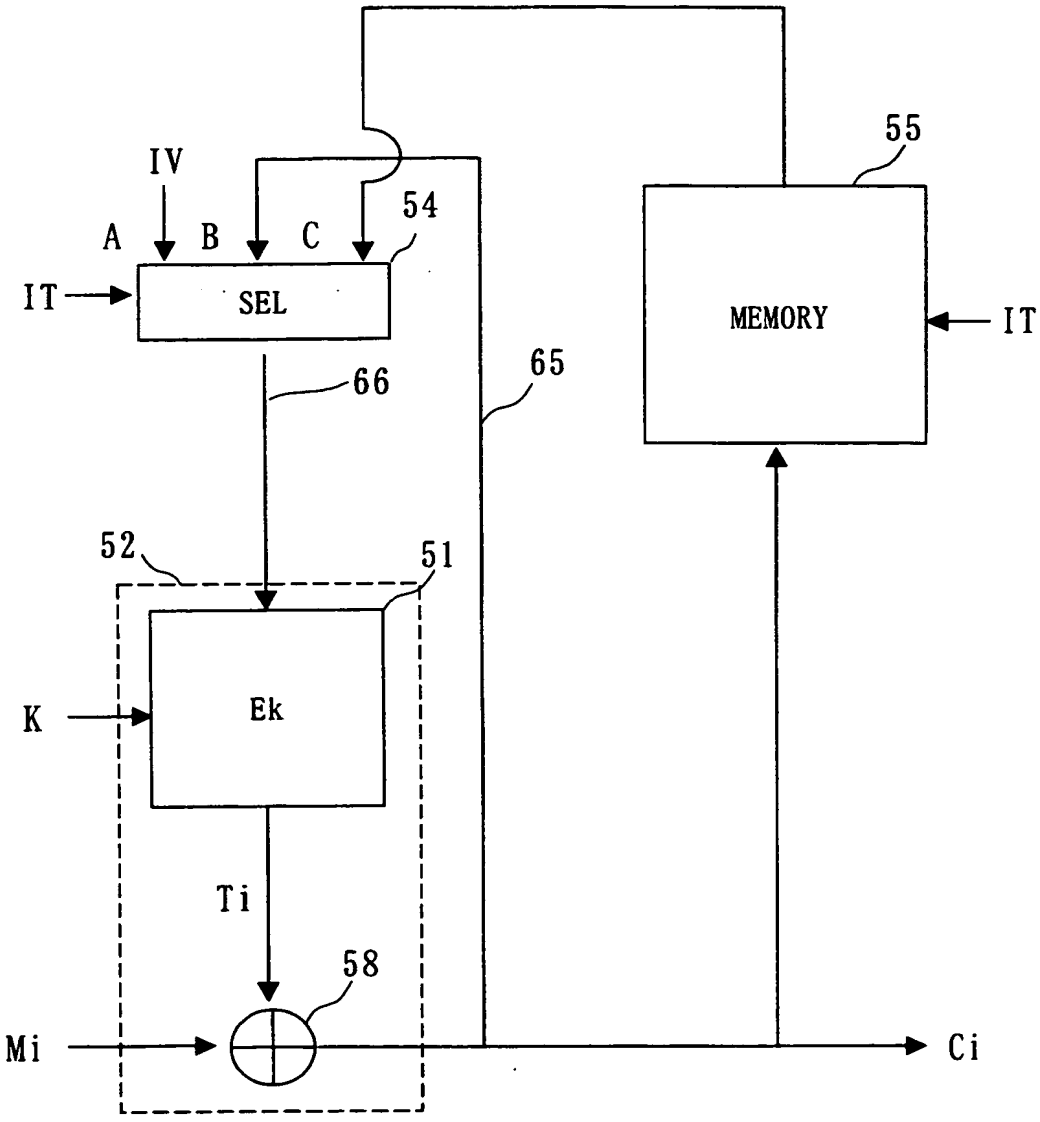


図19

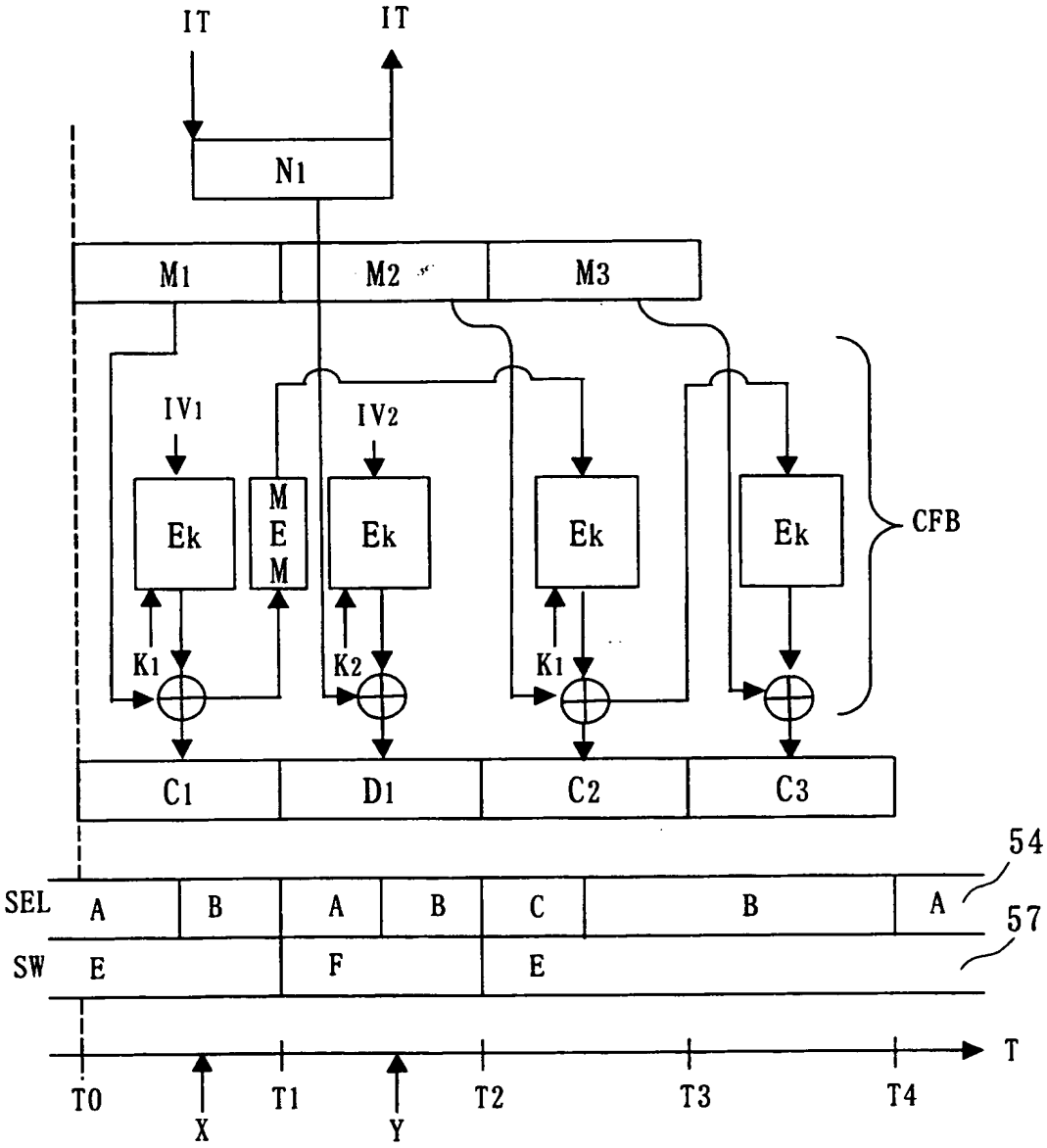

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CFB
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

図20

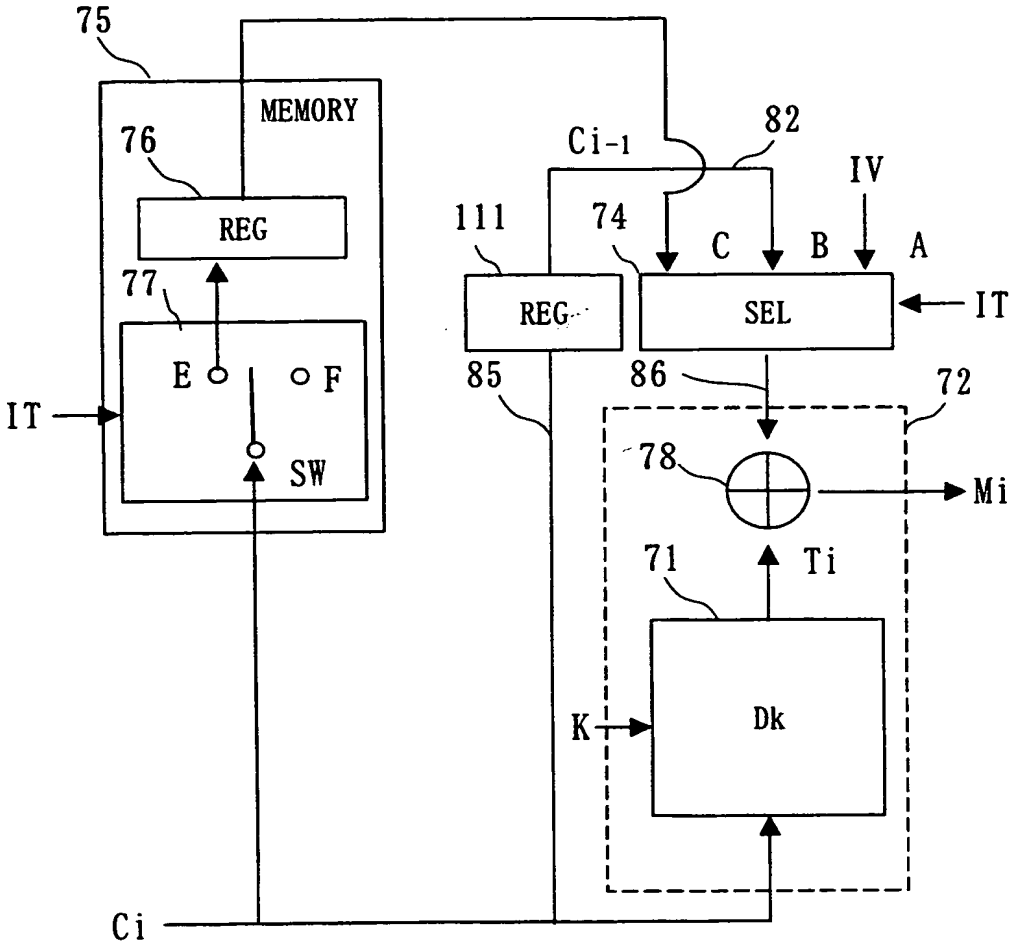

75
MEMORY
76
REG
77
E
F
SW
IT
Ci-1
82
IV
111
74
C
B
A
REG
SEL
IT
85
86
72
78
Mi
71
Ti
K
Dk
Ci

図21

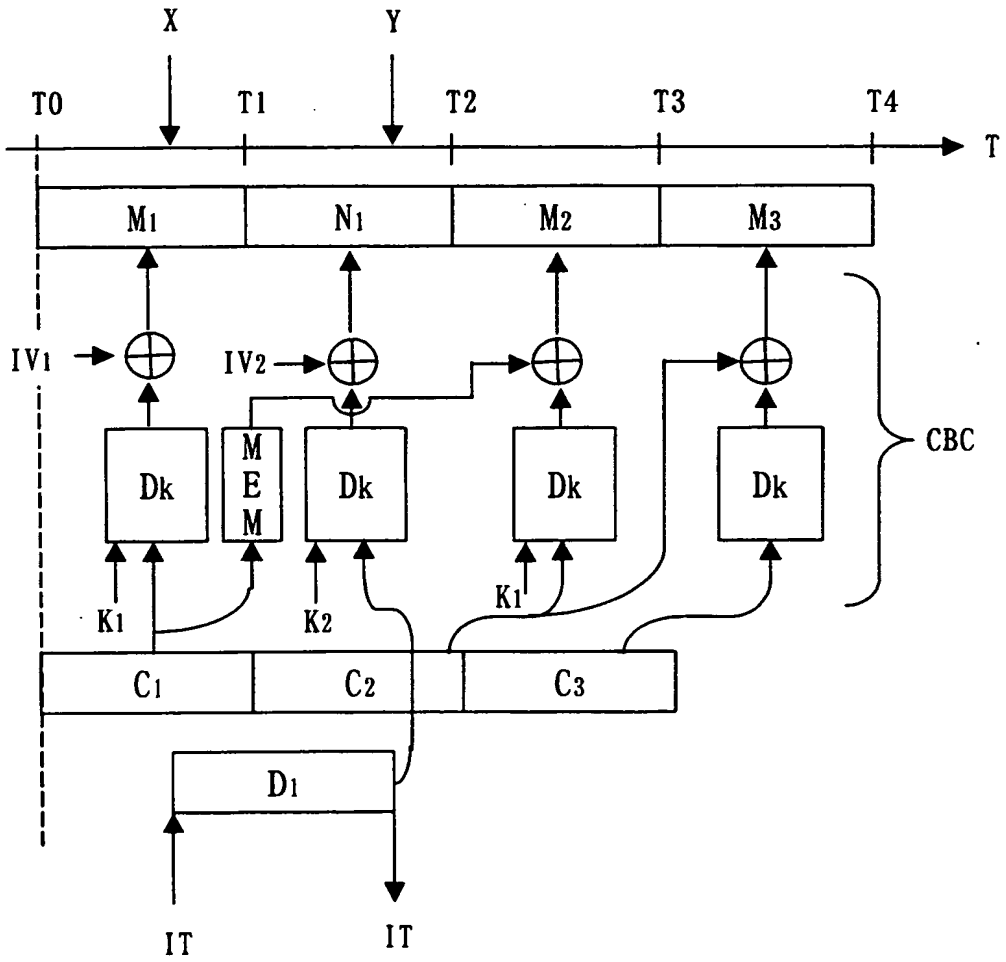

X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
IV1
IV2
Dk
MEM
Dk
Dk
Dk
CBC
K1
K2
K1
C1
C2
C3
D1
IT
IT

図22

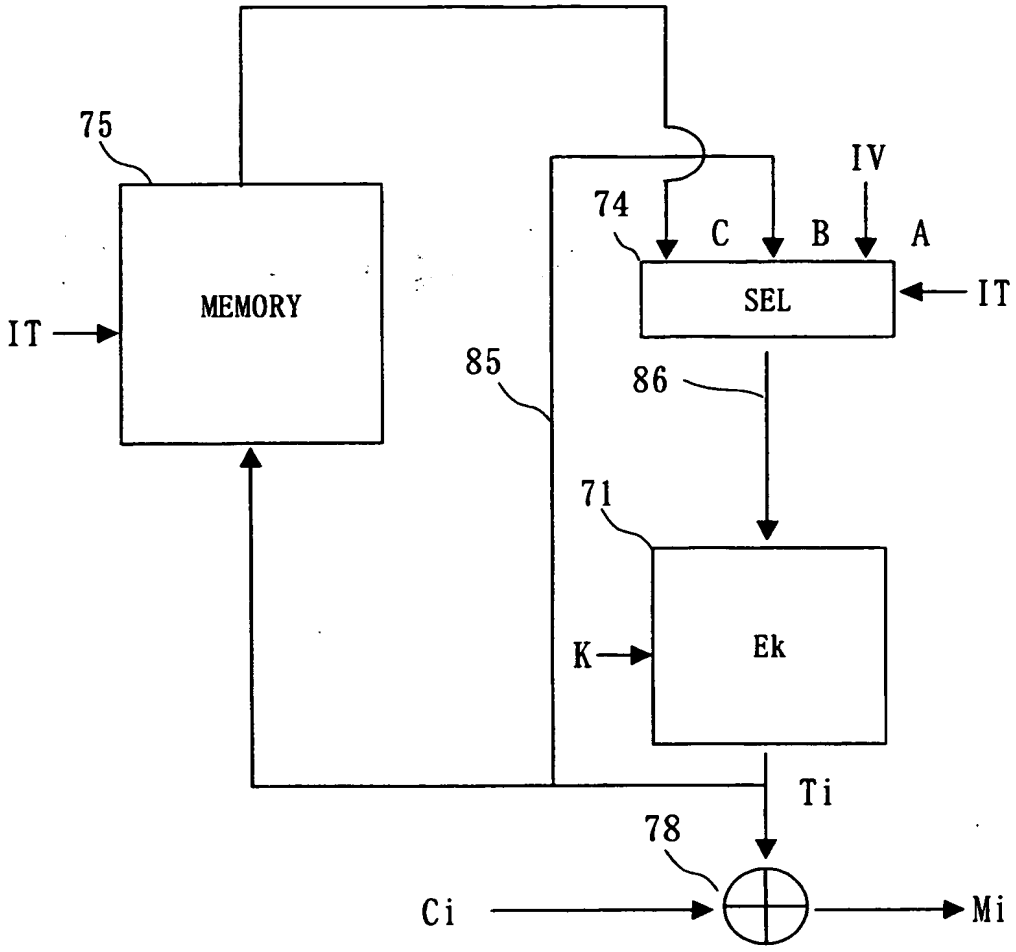


図23

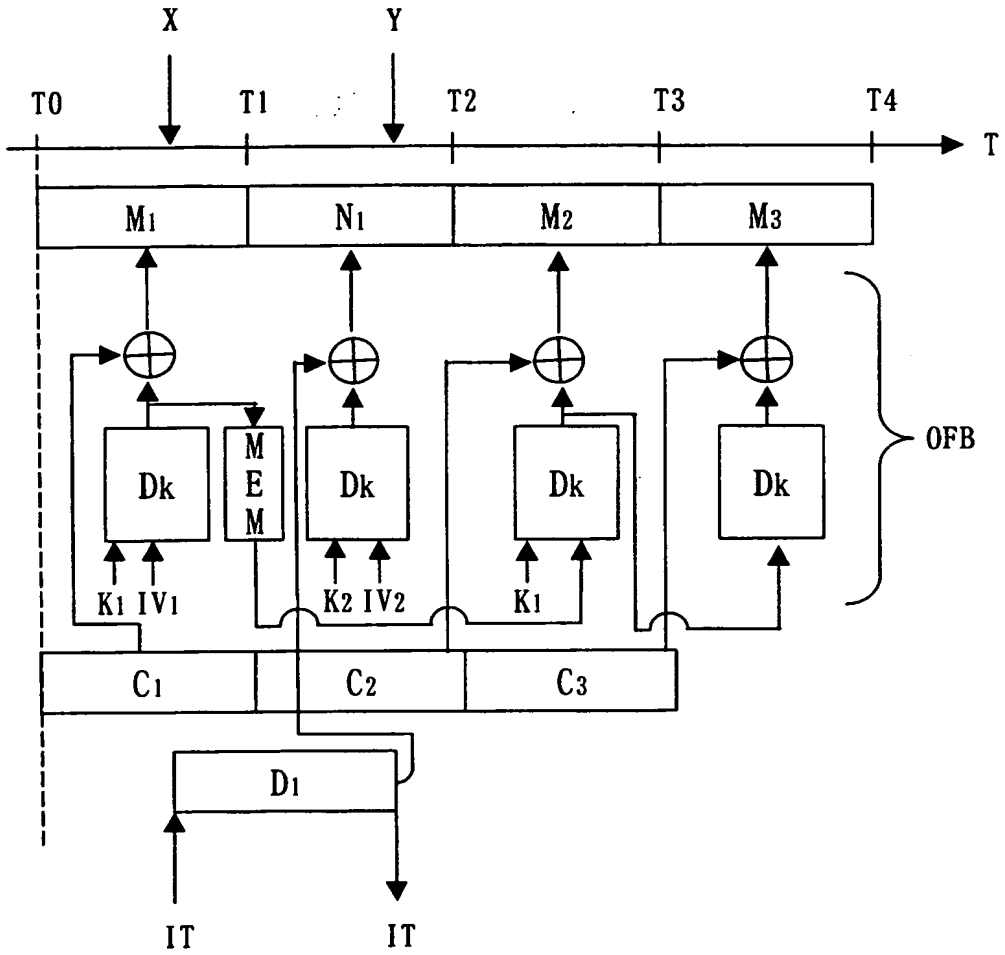

X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
Dk
MEM
Dk
Dk
Dk
OFB
K1 IV1
K2 IV2
K1
C1
C2
C3
D1
IT
IT

図24

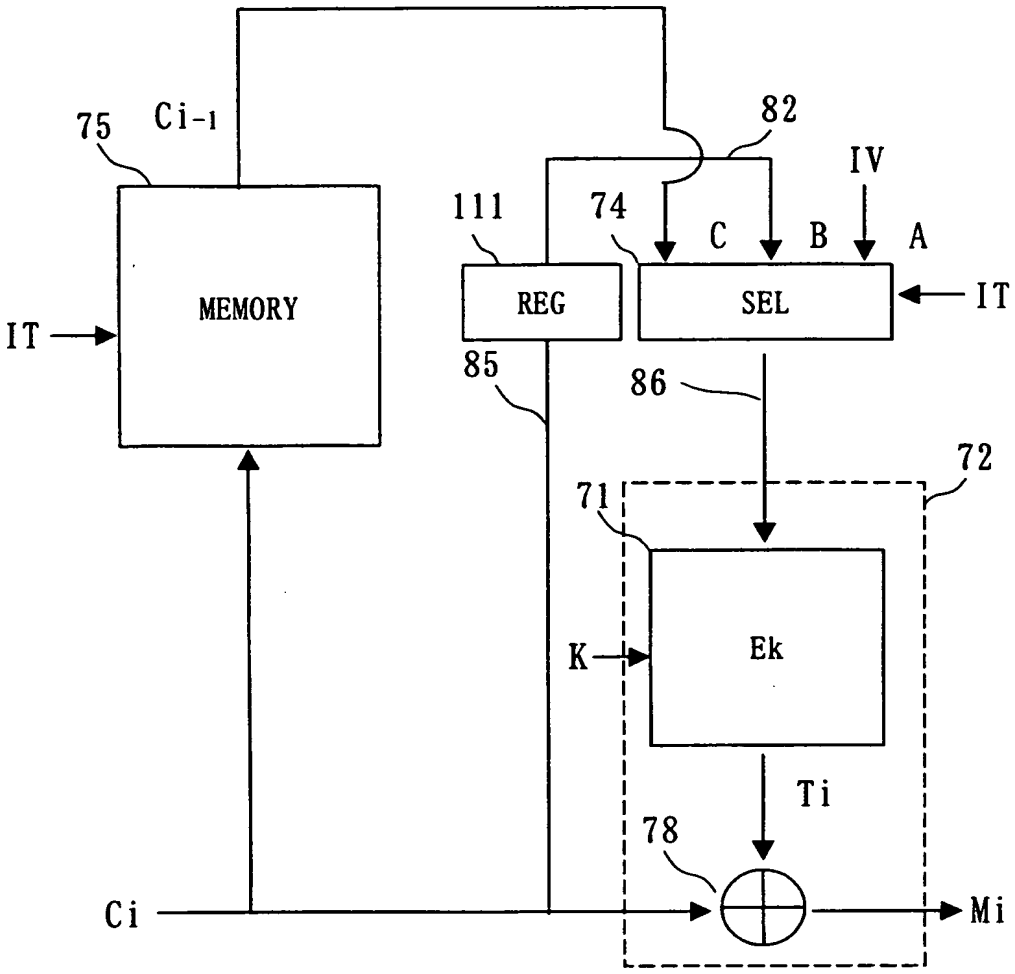

75
Ci-1
82
IV
111
74
C
B
A
MEMORY
REG
SEL
IT
IT
85
86
72
71
K
Ek
Ti
78
Ci
Mi

図25

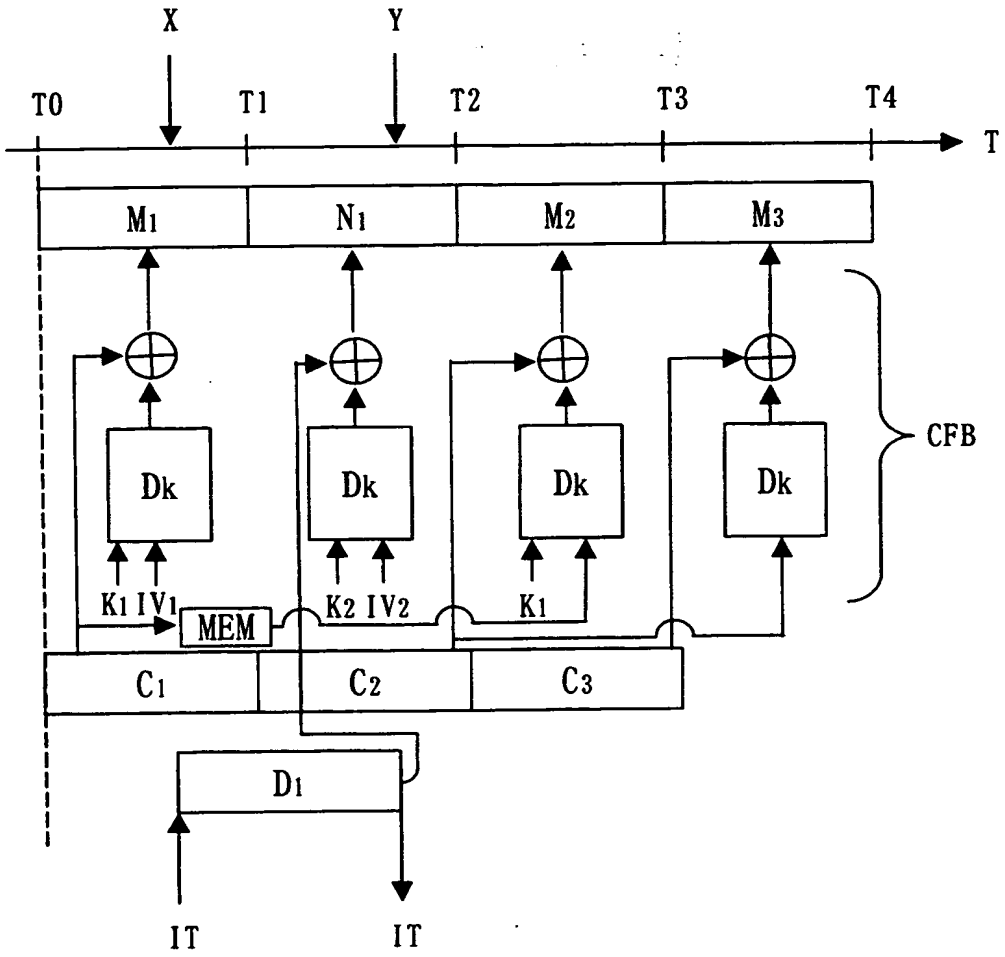

X
Y
T0
T1
T2
T3
T4
T
M1
N1
M2
M3
Dk
Dk
Dk
Dk
CFB
K1 IV1
MEM
K2 IV2
K1
C1
C2
C3
D1
IT
IT

図26

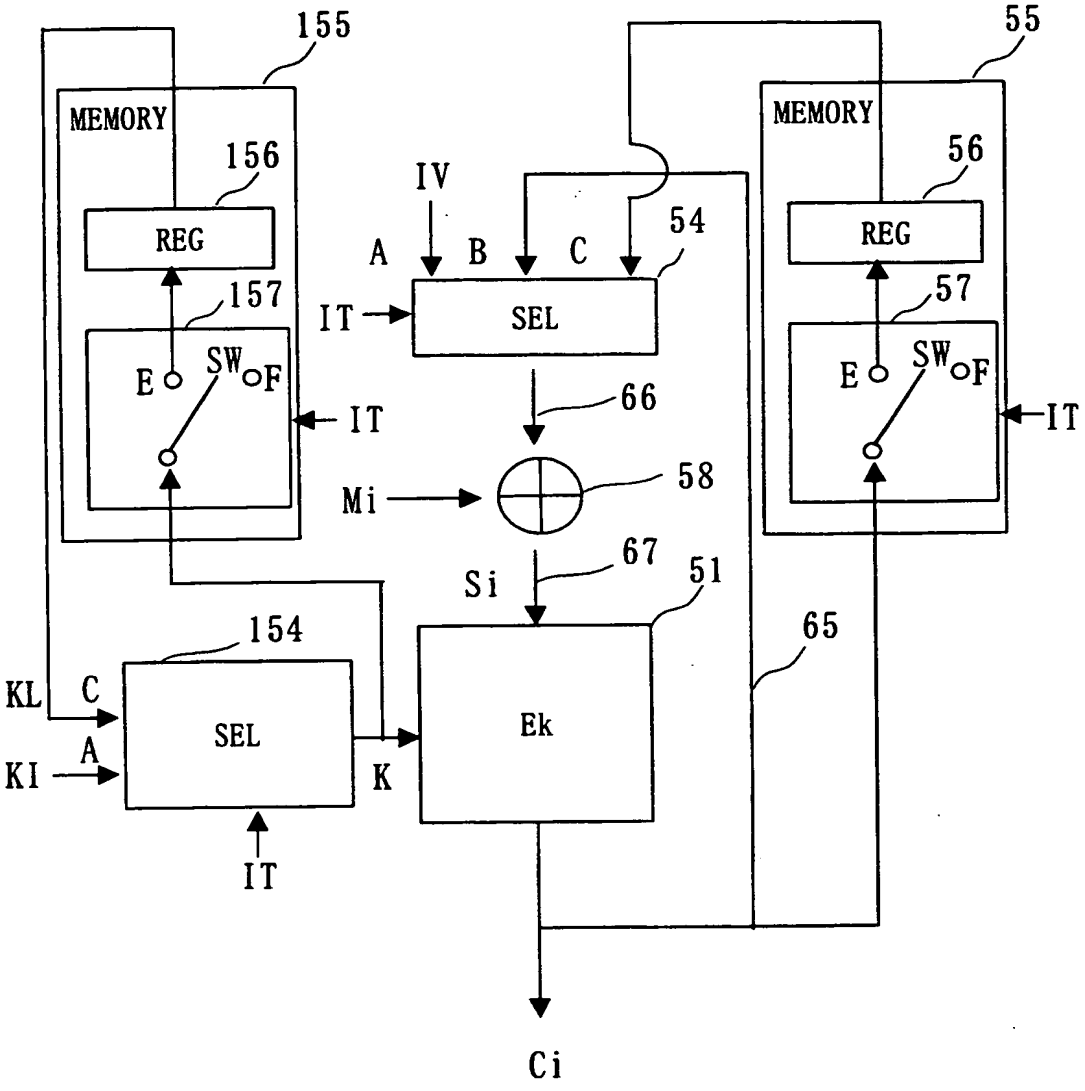

155
MEMORY
156
REG
157
E
SW
F
IT
IV
A
B
C
54
IT
SEL
66
Mi
58
67
Si
51
154
KL
C
A
KI
SEL
K
Ek
65
IT
55
MEMORY
56
REG
57
E
SW
F
IT
Ci

図27

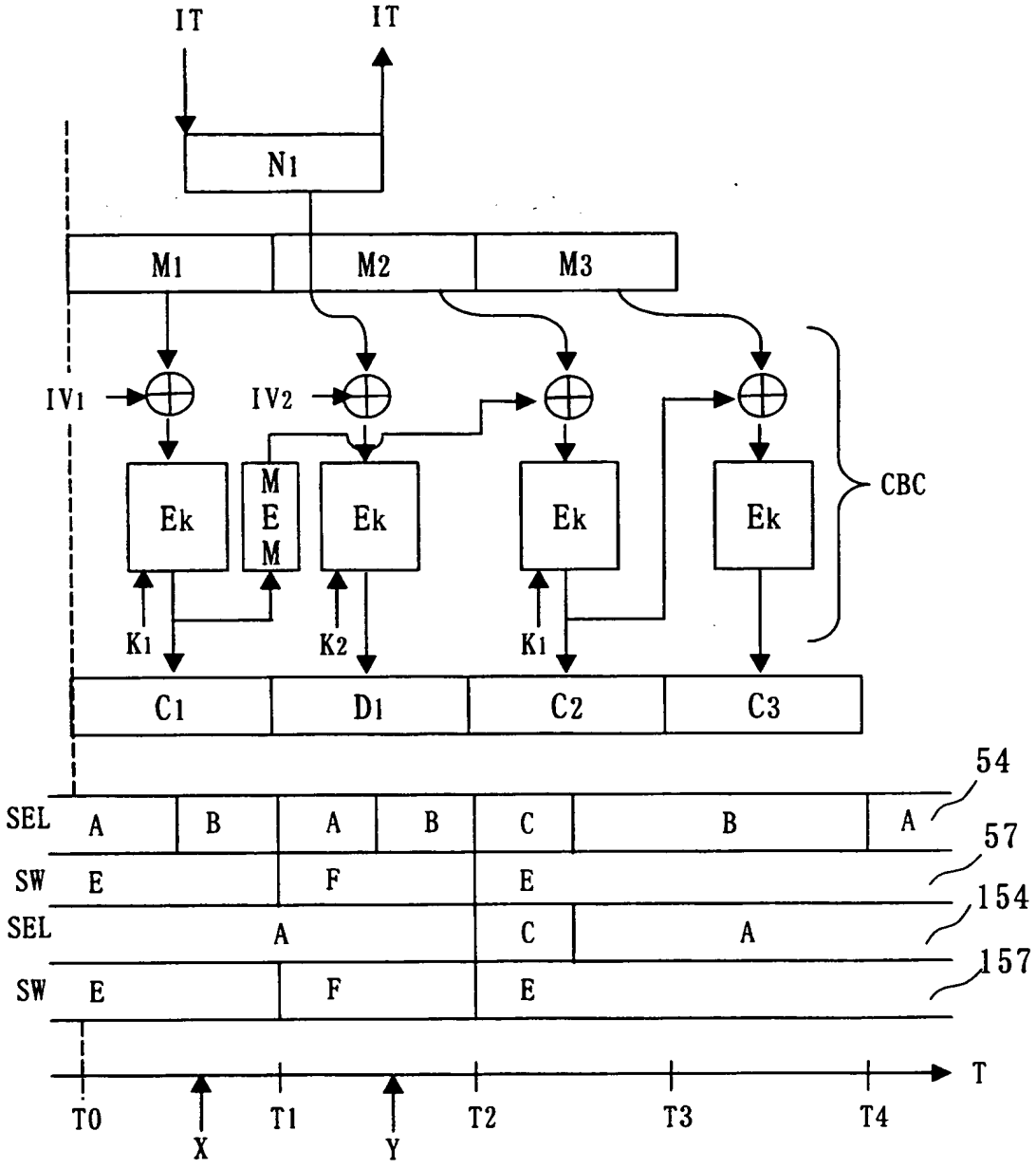

IT
IT
N1
M1
M2
M3
IV1
IV2
Ek
MEM
Ek
Ek
Ek
CBC
K1
K2
K1
C1
D1
C2
C3
54
SEL
A
B
A
B
C
B
A
57
SW
E
F
E
154
SEL
A
C
A
157
SW
E
F
E
T
T0
X
T1
Y
T2
T3
T4

図28

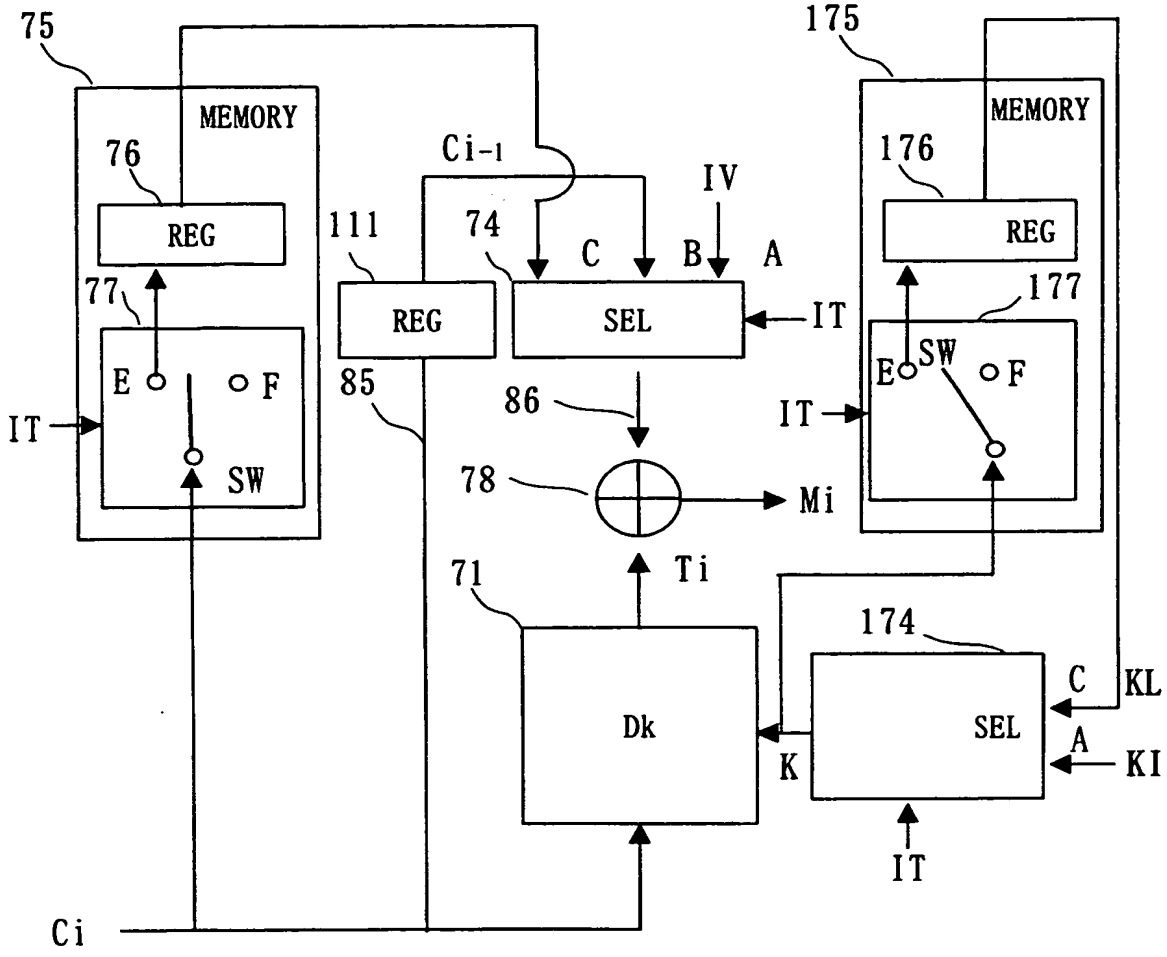

75
MEMORY
76
REG
77
E
F
SW
IT
Ci-1
111
REG
74
C
B
A
IV
SEL
IT
85
86
78
Mi
Ti
71
Dk
K
Ci
175
MEMORY
176
REG
177
E
SW
F
IT
174
C
KL
SEL
A
KI
IT

図29

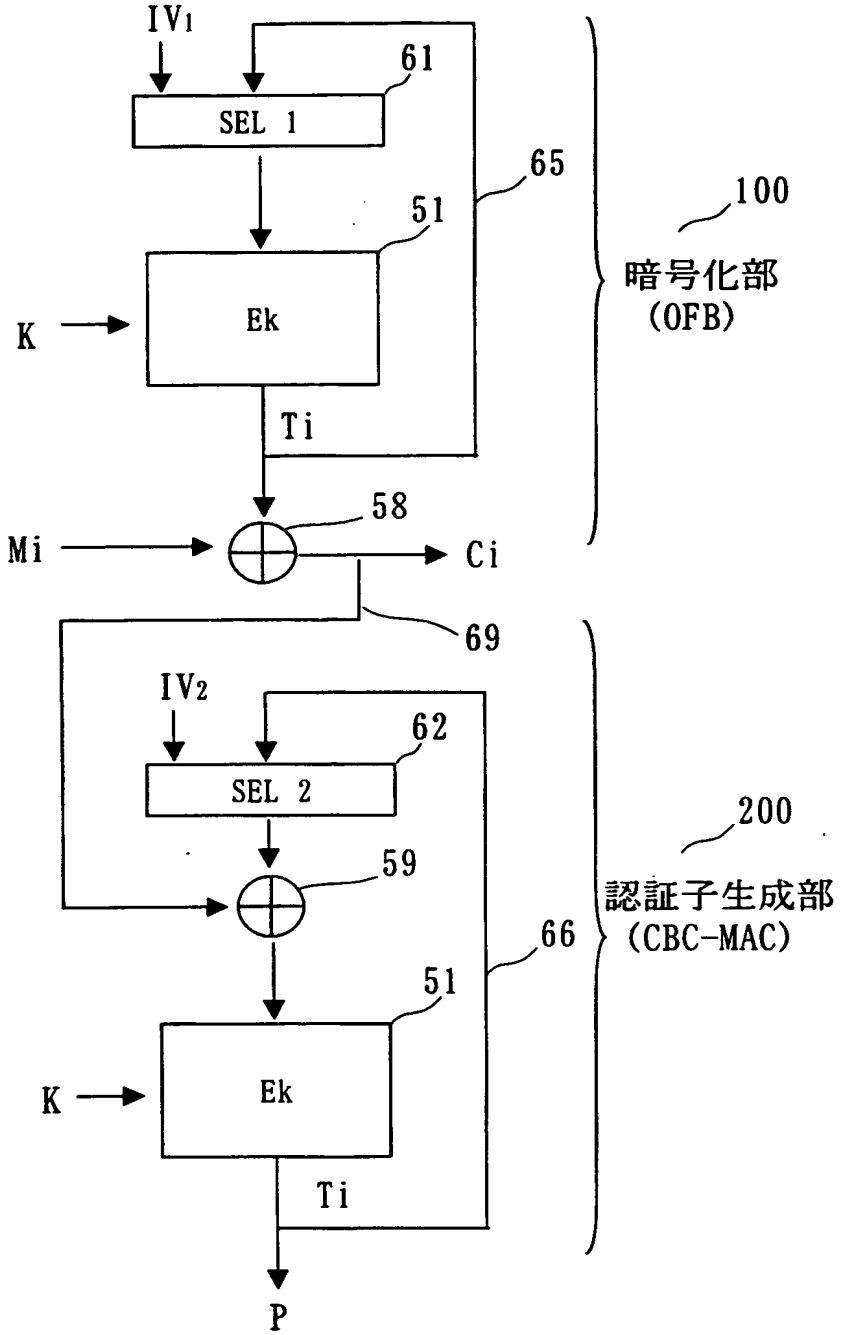

IV1
61
SEL 1
65
51
100
暗号化部
(OFB)
K
Ek
Ti
58
Mi
Ci
69
IV2
62
SEL 2
200
59
認証子生成部
(CBC-MAC)
66
51
K
Ek
Ti
P

図30

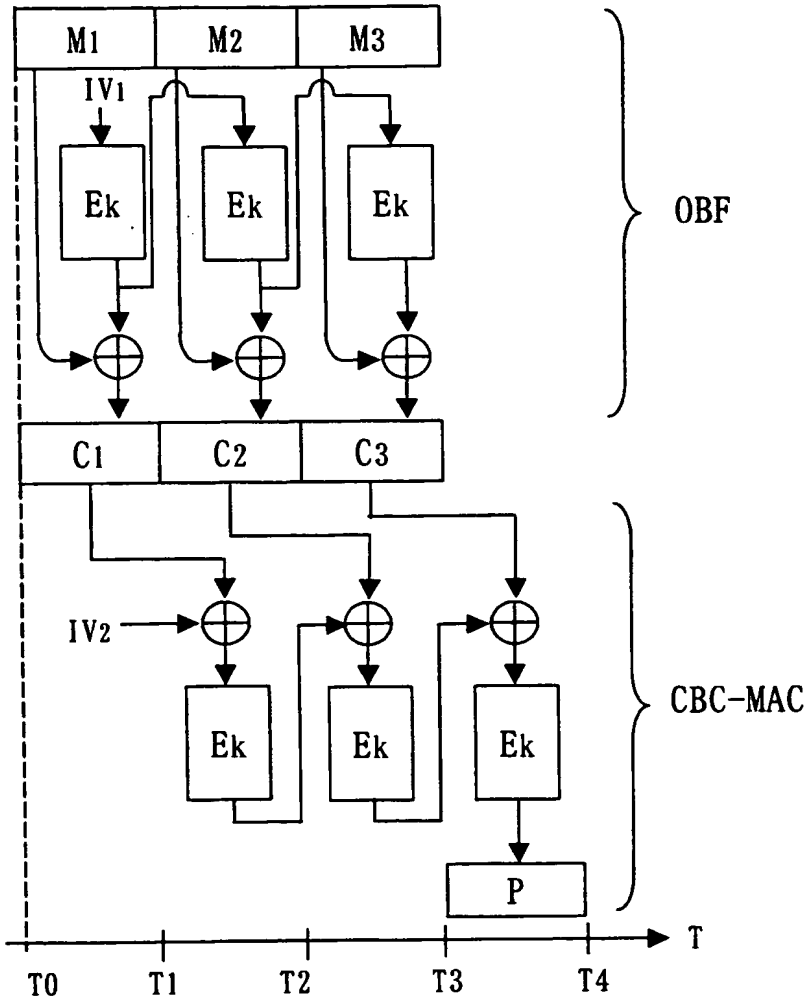

M1
M2
M3
IV1
Ek
Ek
Ek
OBF
C1
C2
C3
IV2
Ek
Ek
Ek
CBC-MAC
P
T
T0
T1
T2
T3
T4

図31

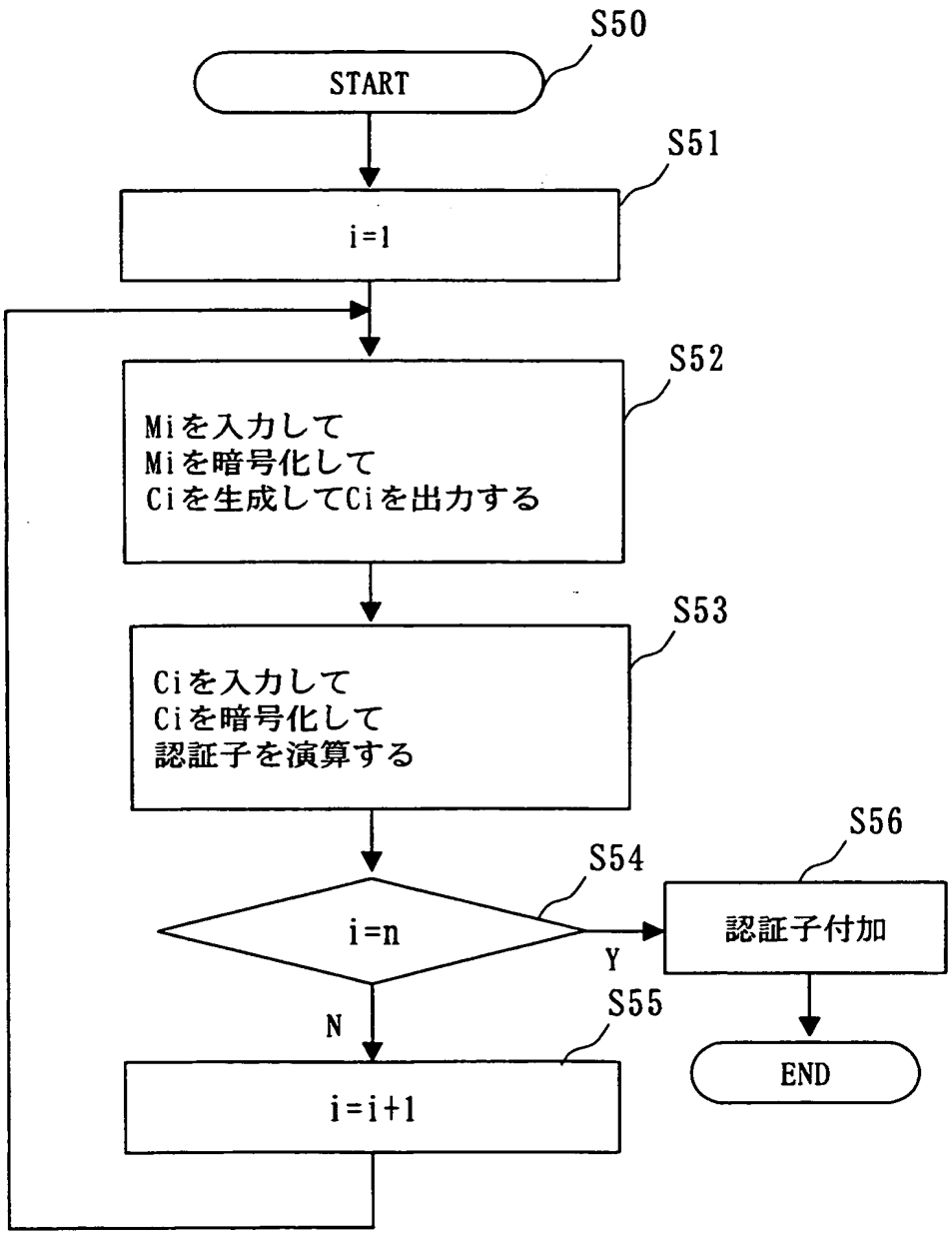

S50
START
S51
i=1
S52
Miを入力して
Miを暗号化して
Ciを生成してCiを出力する
S53
Ciを入力して
Ciを暗号化して
認証子を演算する
S54
i=n
Y
N
S56
認証子付加
END
S55
i=i+1

図32

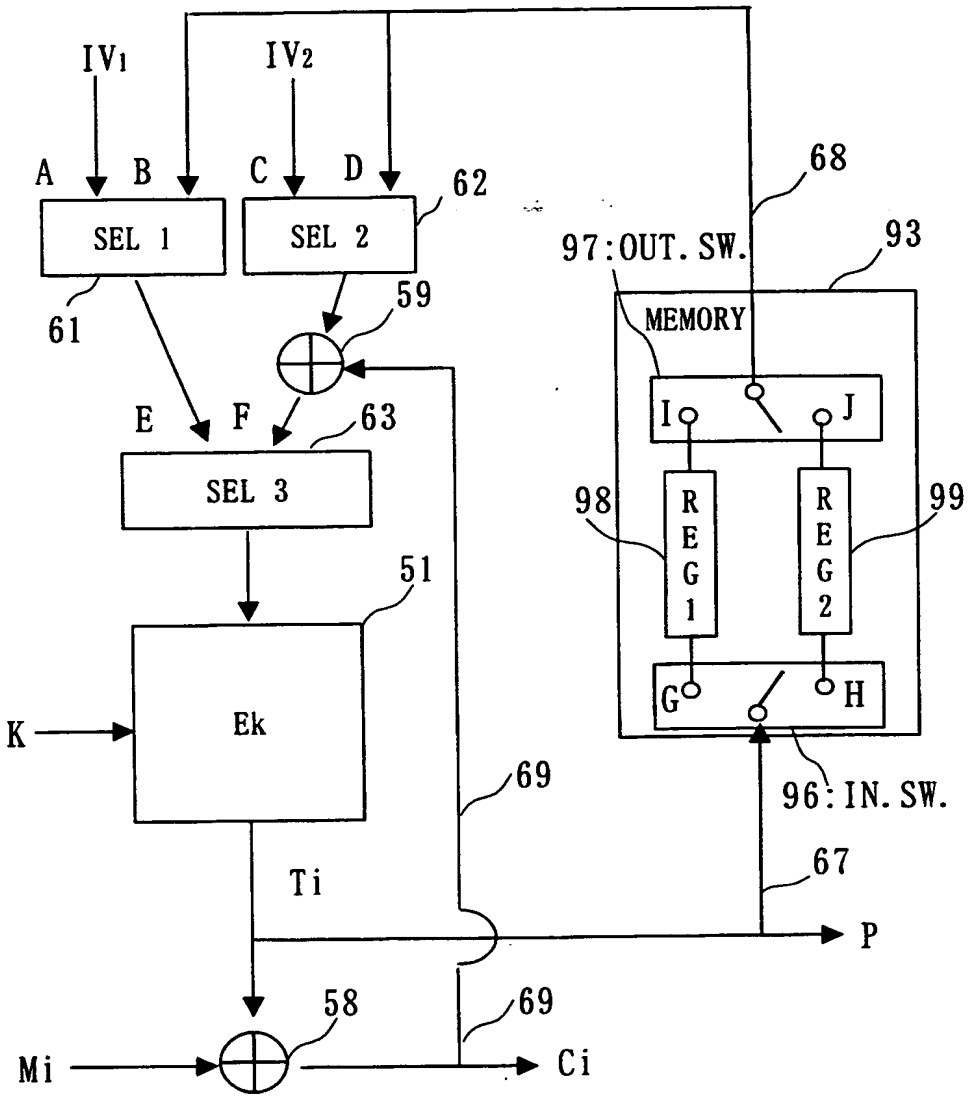

IV1
IV2
A
B
C
D
62
SEL 1
SEL 2
61
59
E
F
63
SEL 3
51
Ek
K
Ti
Mi
58
Ci
69
69
68
97:OUT. SW.
93
MEMORY
I
J
98
REG1
REG2
99
G
H
96:IN. SW.
67
P

図33

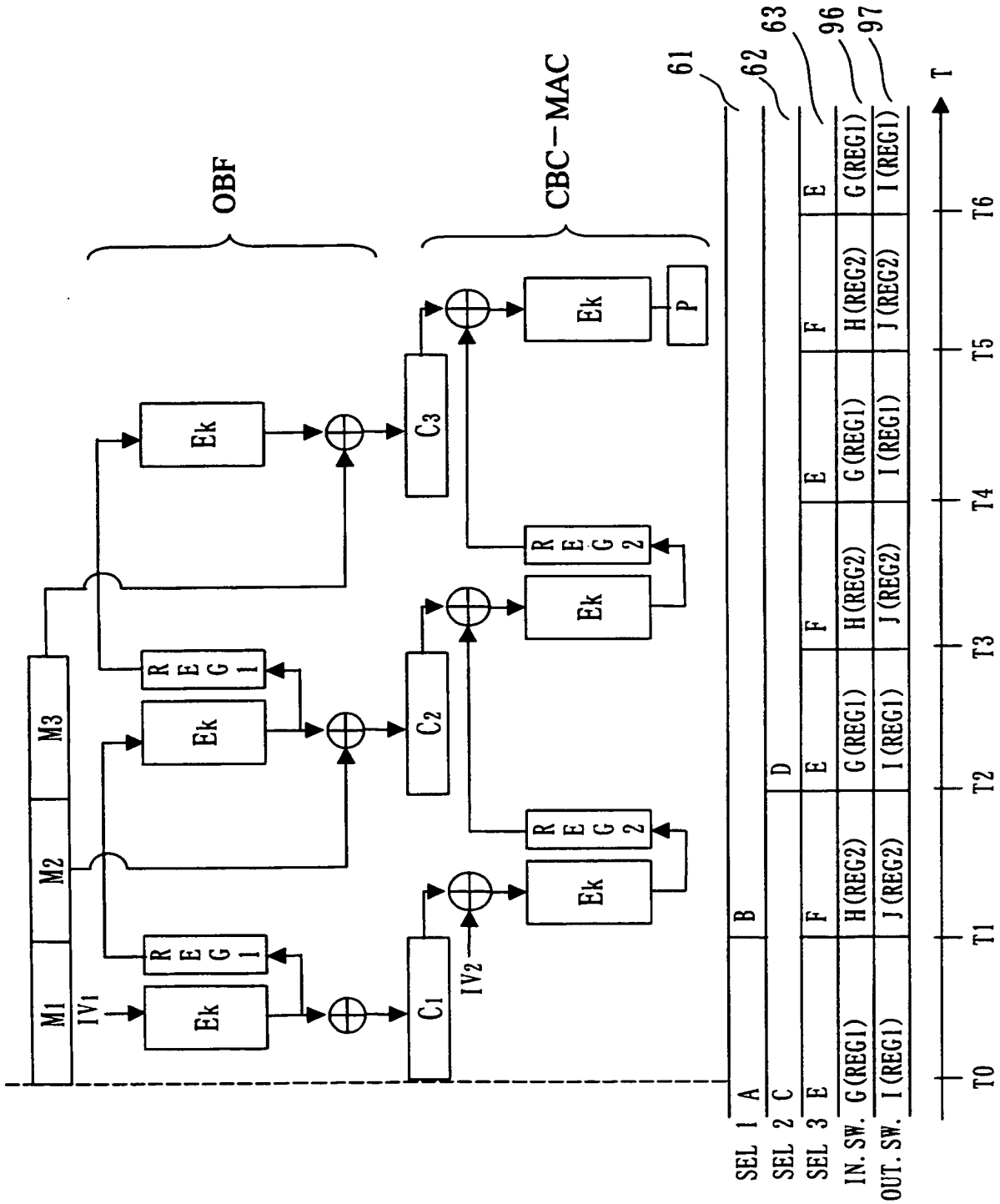

OBF
CBC−MAC
M1
M2
M3
IV1
IV2
Ek
REG1
REG2
C1
C2
C3
P
61
62
63
96
97
T
T0
T1
T2
T3
T4
T5
T6
SEL 1
SEL 2
SEL 3
IN. SW.
OUT. SW.
A
B
C
D
E
F
G(REG1)
H(REG2)
I(REG1)
J(REG2)

図34

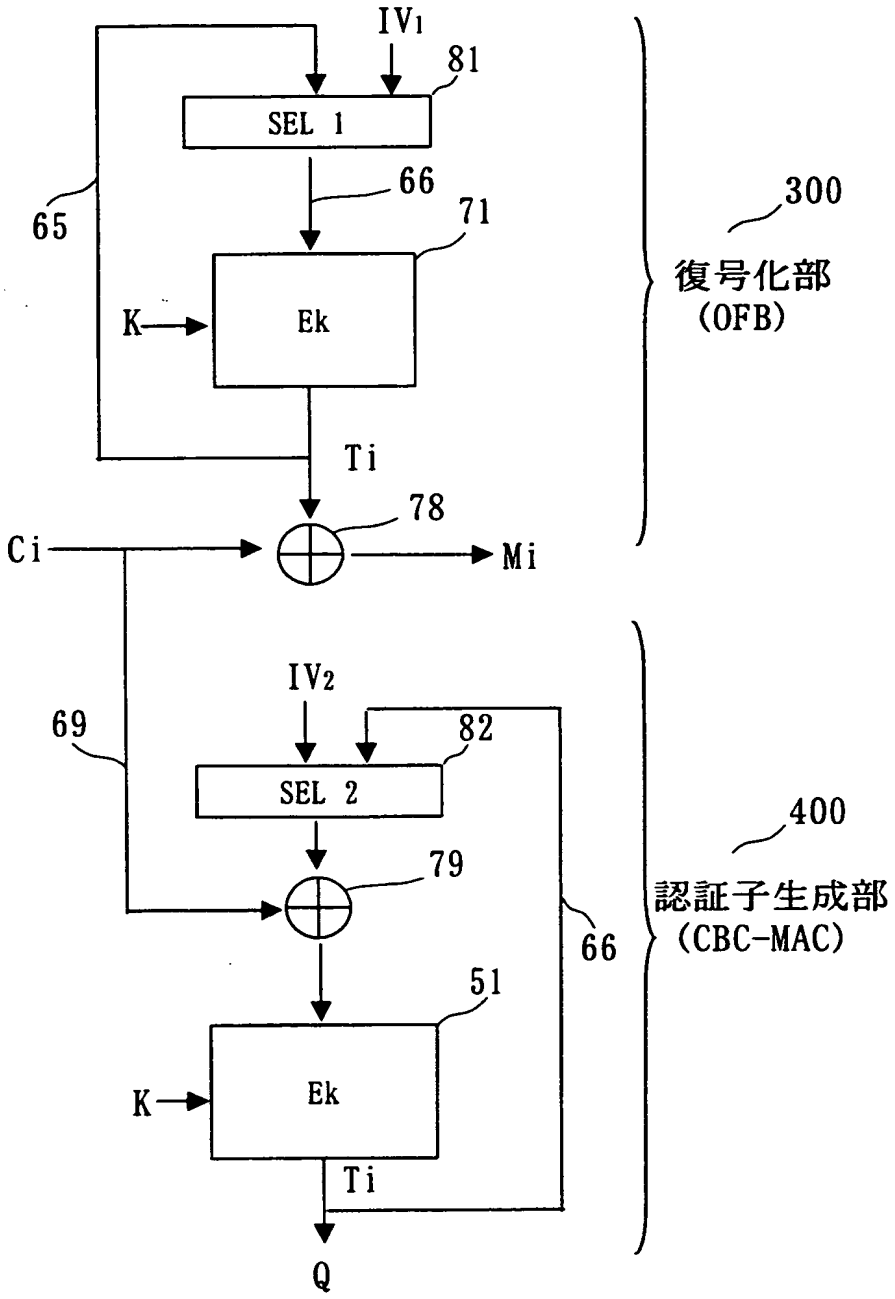

IV1
81
SEL 1
66
65
71
K
Ek
300
復号化部
(OFB)
Ti
78
Ci
Mi
IV2
69
82
SEL 2
400
79
認証子生成部
(CBC-MAC)
66
51
K
Ek
Ti
Q

図35

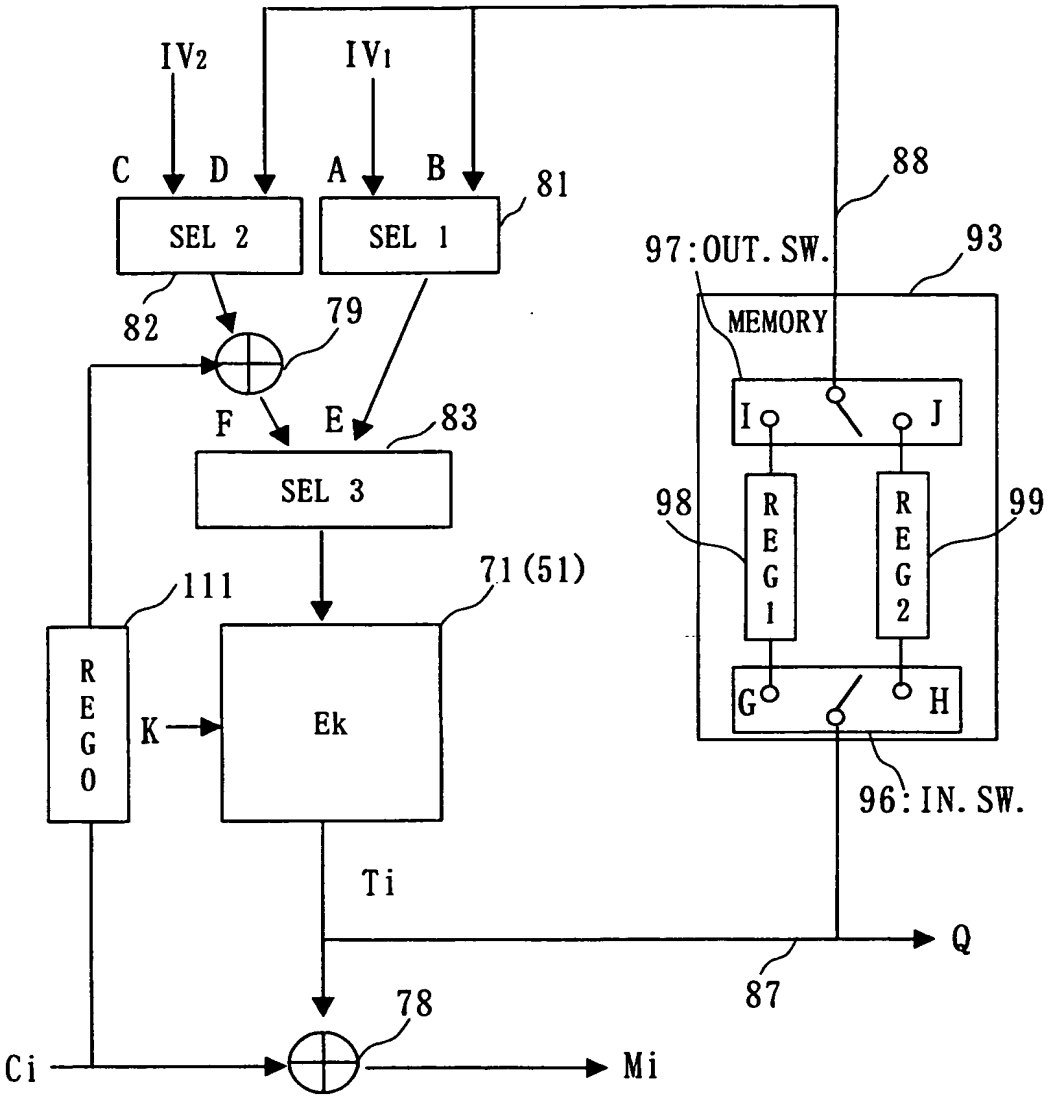

IV2
IV1
C
D
A
B
81
SEL 2
SEL 1
82
79
F
E
83
SEL 3
111
71(51)
REG0
K
Ek
Ti
78
Ci
Mi
88
97:OUT. SW.
93
MEMORY
I
J
98
REG1
REG2
99
G
H
96:IN. SW.
Q
87

図 36

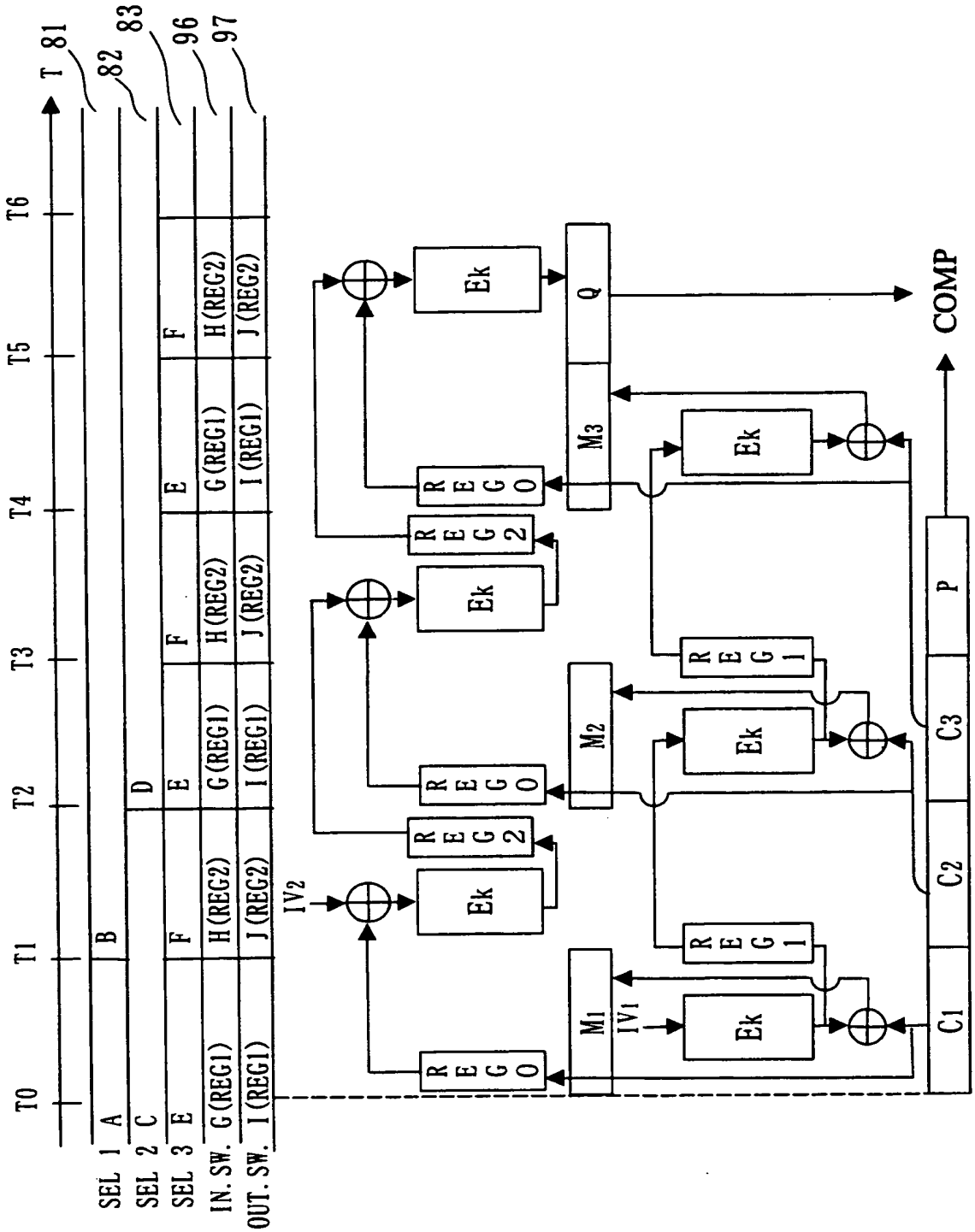

T 81
82
83
96
97
T0
T1
T2
T3
T4
T5
T6
SEL 1 A B
SEL 2 C D
SEL 3 E F E F E F
IN. SW. G(REG1) H(REG2) G(REG1) H(REG2) G(REG1) H(REG2)
OUT. SW. I(REG1) J(REG2) I(REG1) J(REG2) I(REG1) J(REG2)
IV2
IV1
Ek
REG 0
REG 1
REG 2
M1
M2
M3
Q
P
C1
C2
C3
COMP

図37

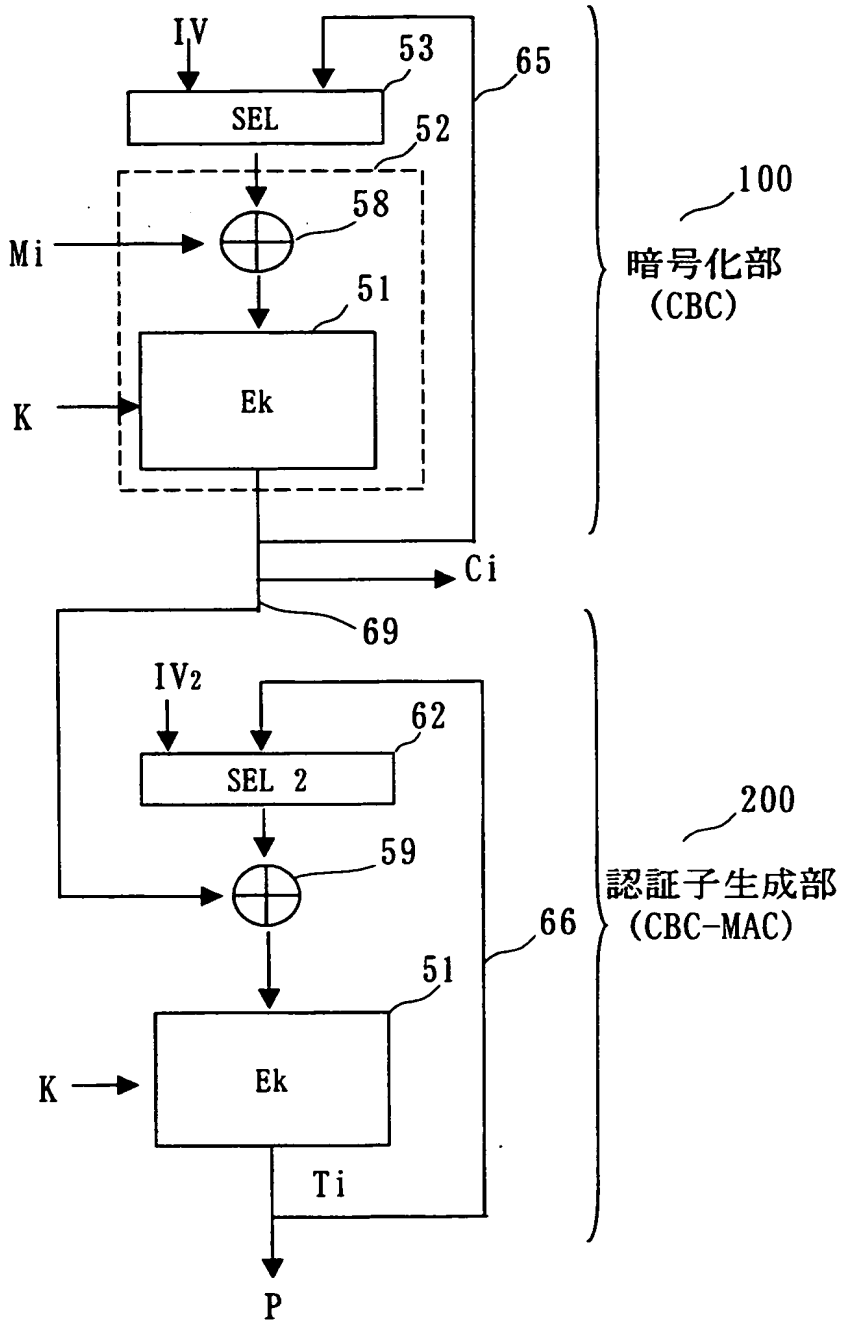

IV
53
65
SEL
52
100
58
Mi
51
暗号化部
(CBC)
Ek
K
Ci
69
IV2
62
SEL 2
200
59
認証子生成部
(CBC-MAC)
66
51
K
Ek
Ti
P

図38

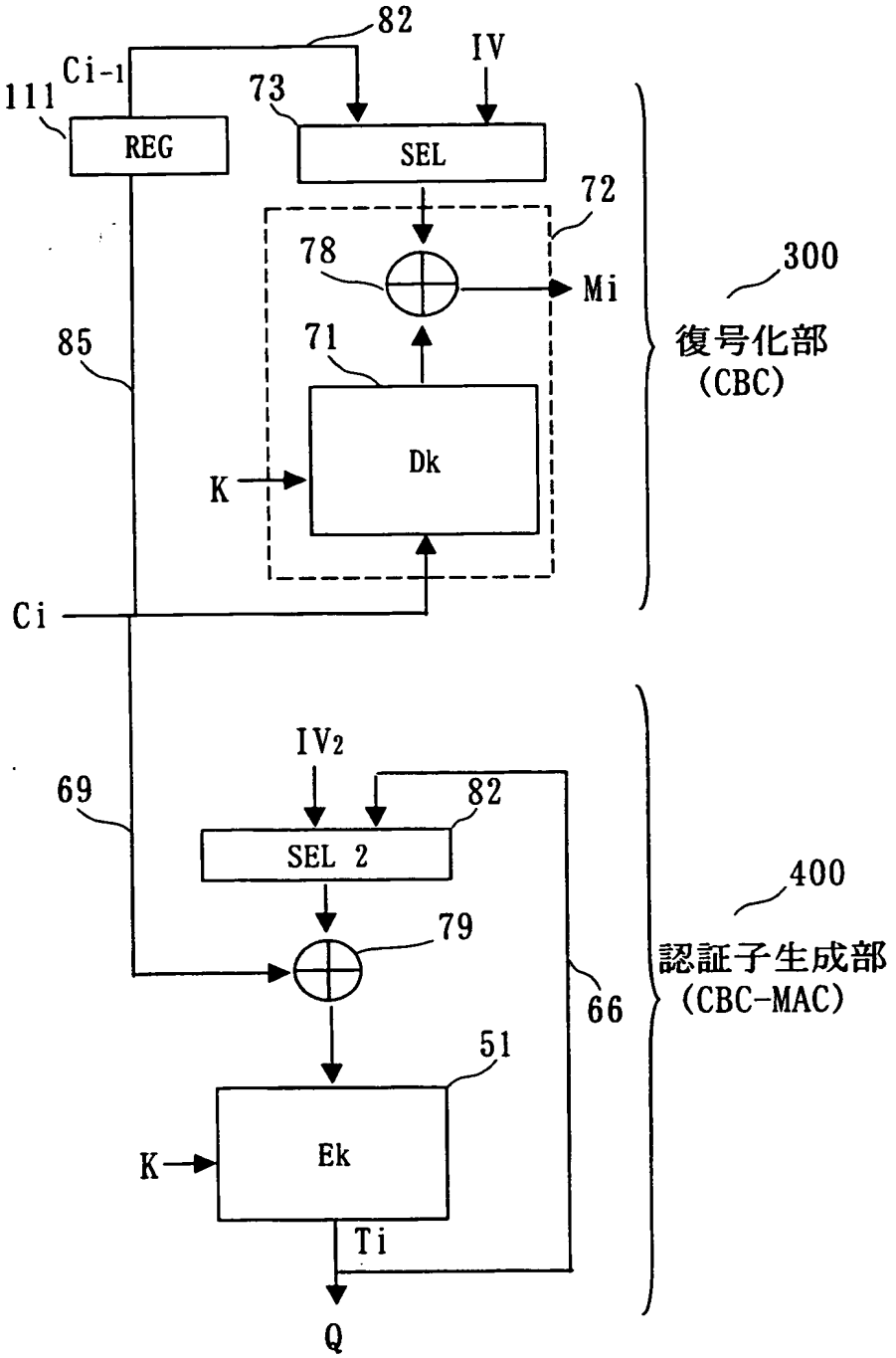

82
IV
Ci-1
111
73
REG
SEL
72
78
Mi
300
85
71
復号化部
(CBC)
Dk
K
Ci
IV2
69
82
SEL 2
400
79
認証子生成部
(CBC-MAC)
66
51
K
Ek
Ti
Q

図39

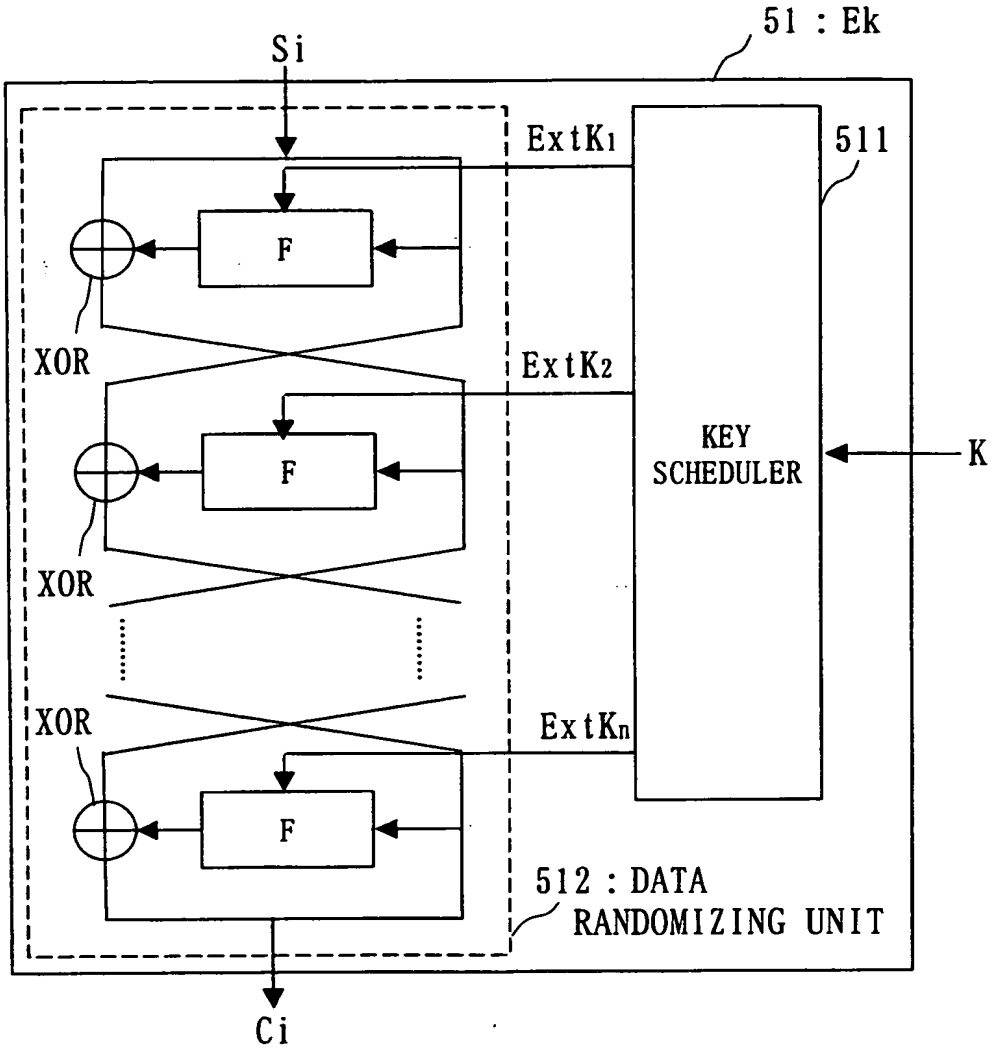

51 : Ek
Si
ExtK1
511
F
XOR
ExtK2
KEY
SCHEDULER
K
F
XOR
XOR
ExtKn
F
512 : DATA
RANDOMIZING UNIT
Ci

図40

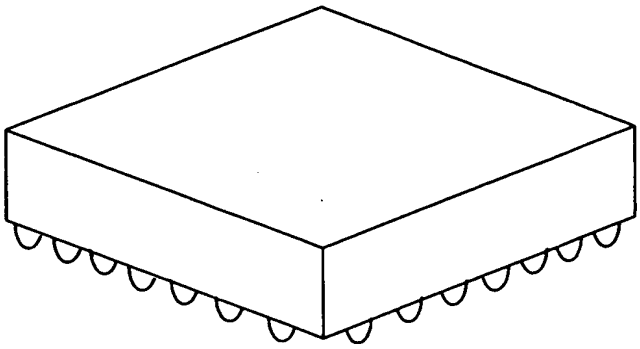


図41

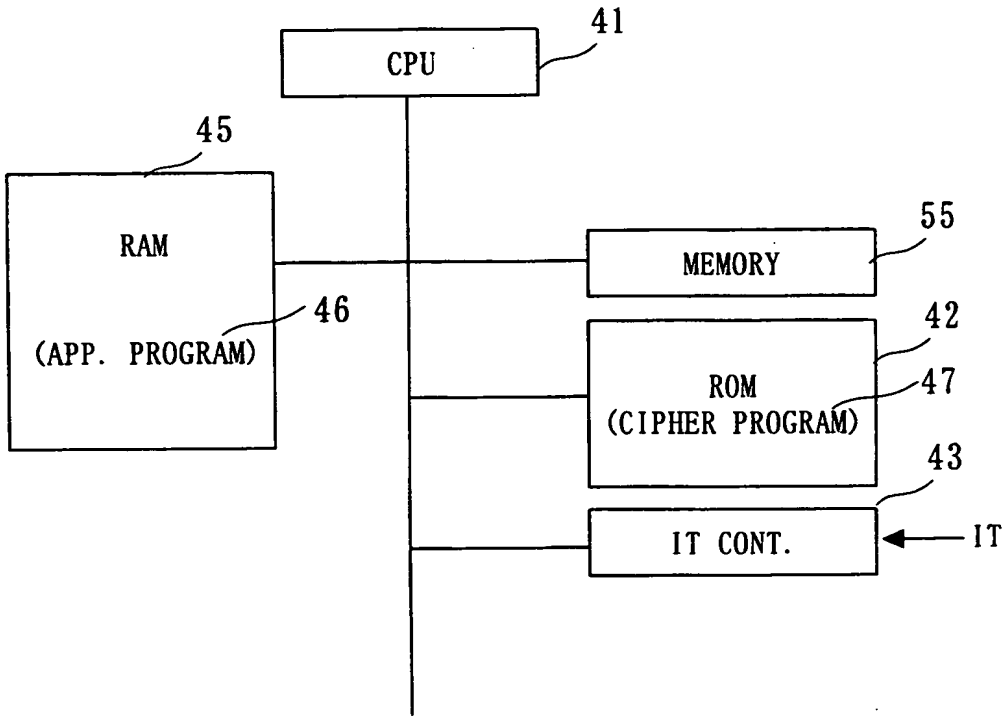

CPU
41
45
RAM
(APP. PROGRAM)
46
MEMORY
55
ROM
(CIPHER PROGRAM)
42
47
IT CONT.
43
IT

図42

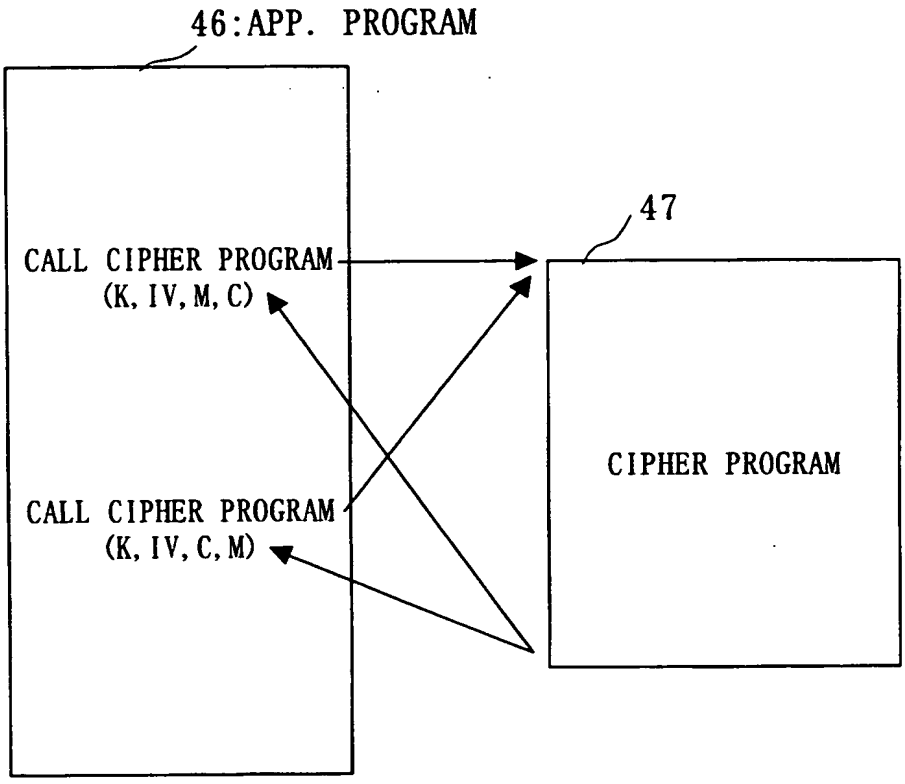

46:APP. PROGRAM
47
CALL CIPHER PROGRAM
(K, IV, M, C)
CALL CIPHER PROGRAM
(K, IV, C, M)
CIPHER PROGRAM

図43

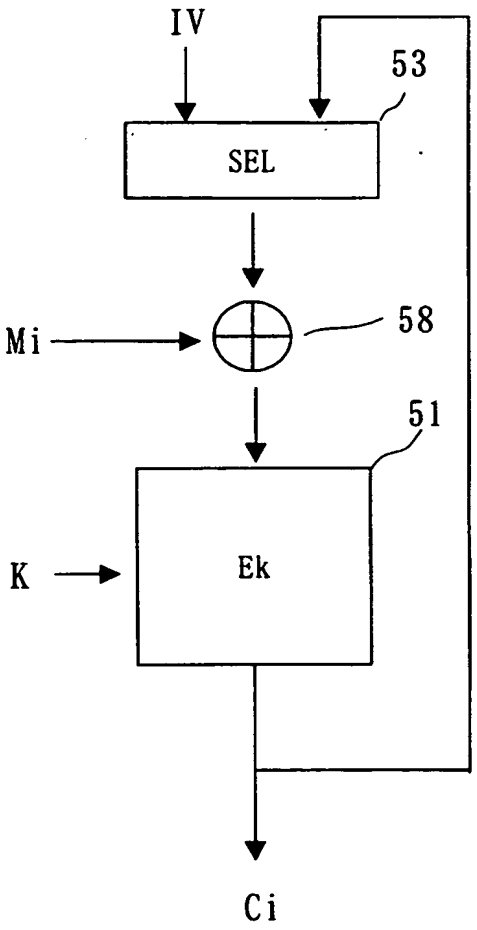


図44

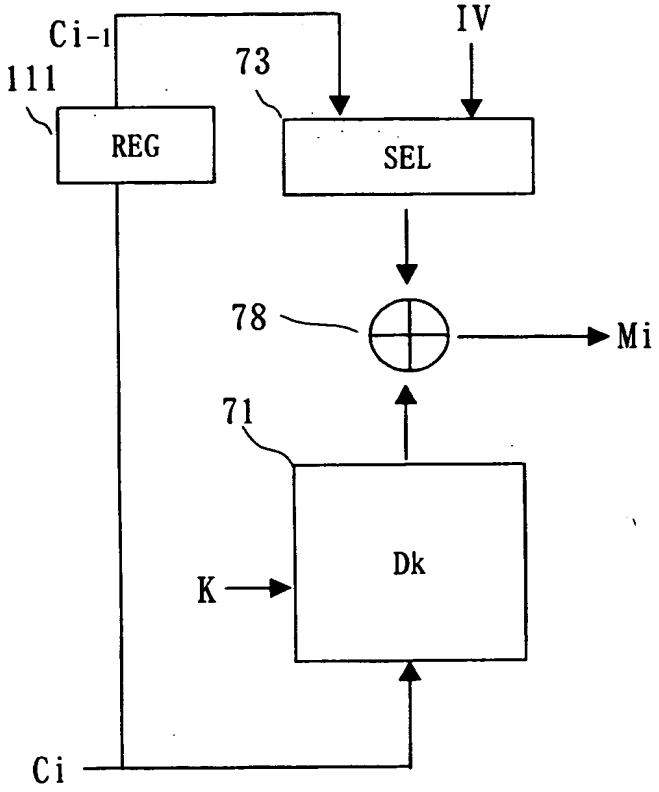


図45

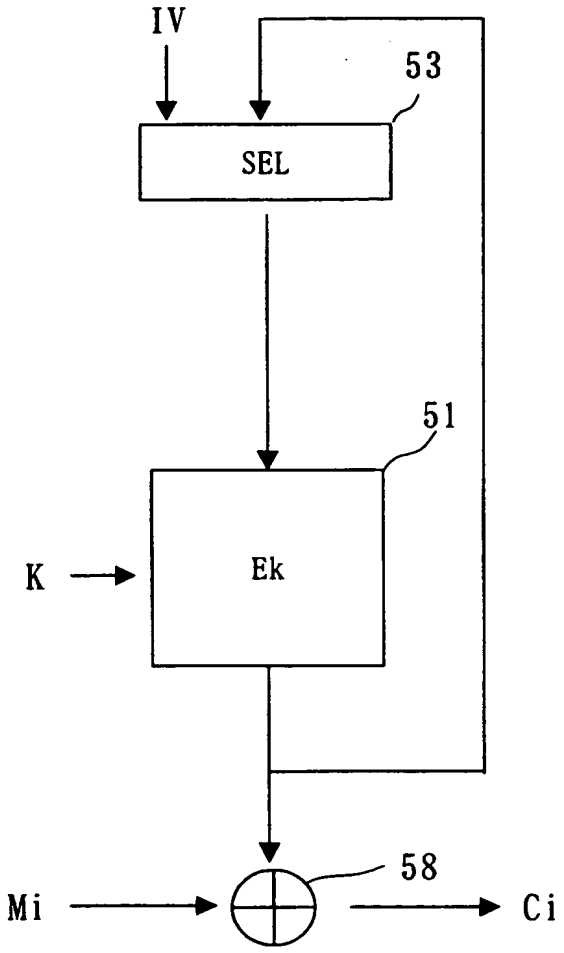


図46

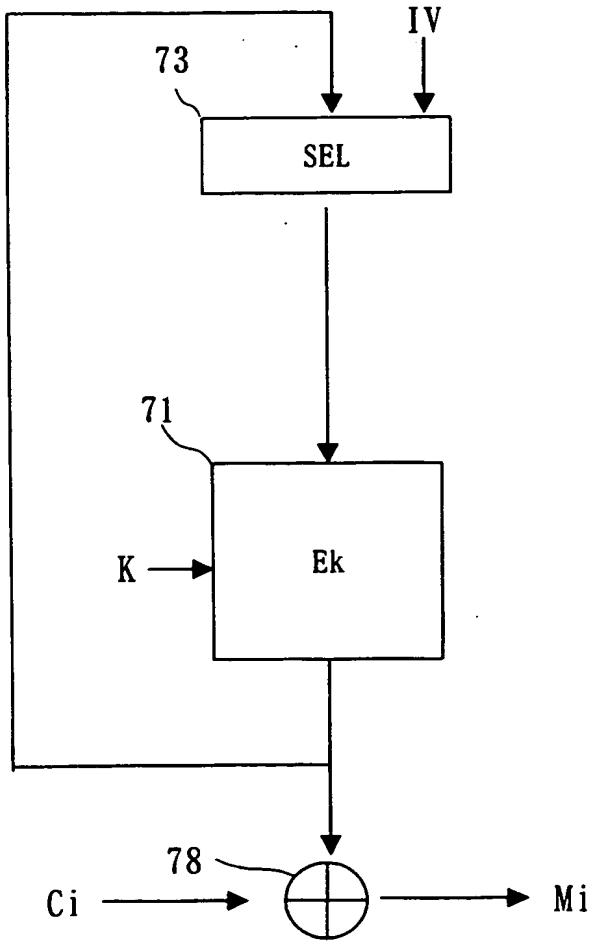


図47

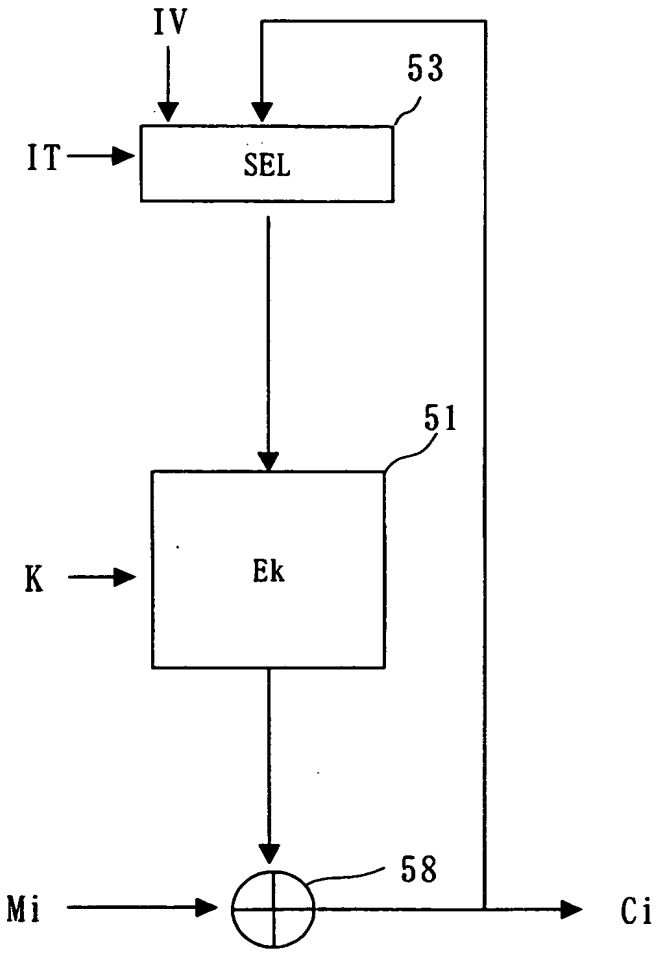


図48

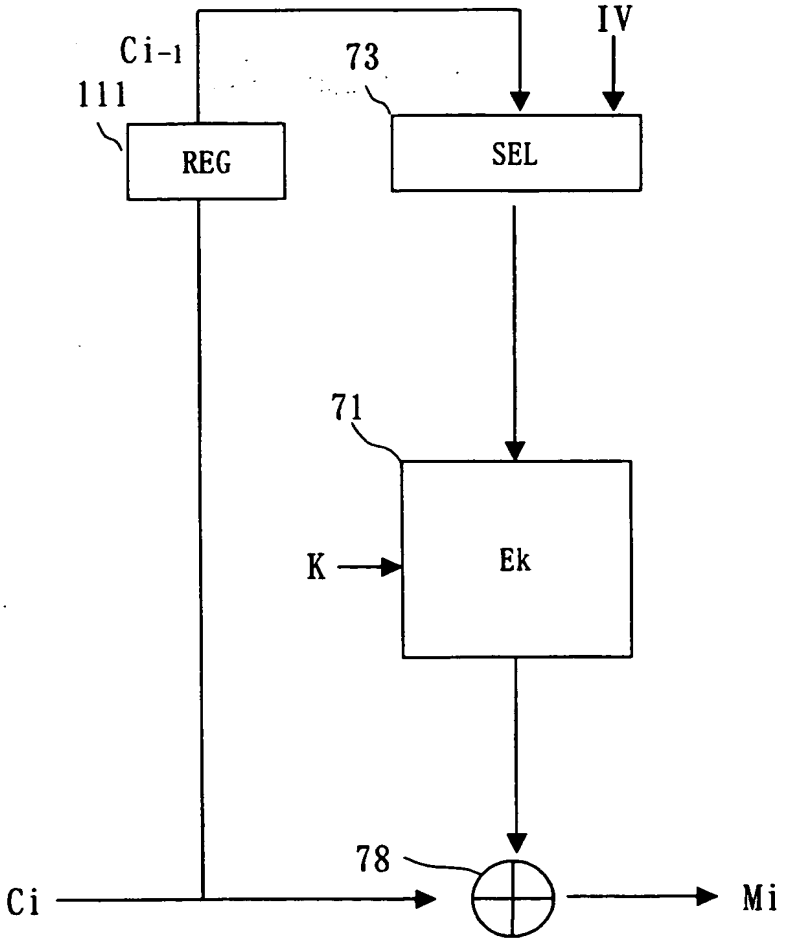


図49

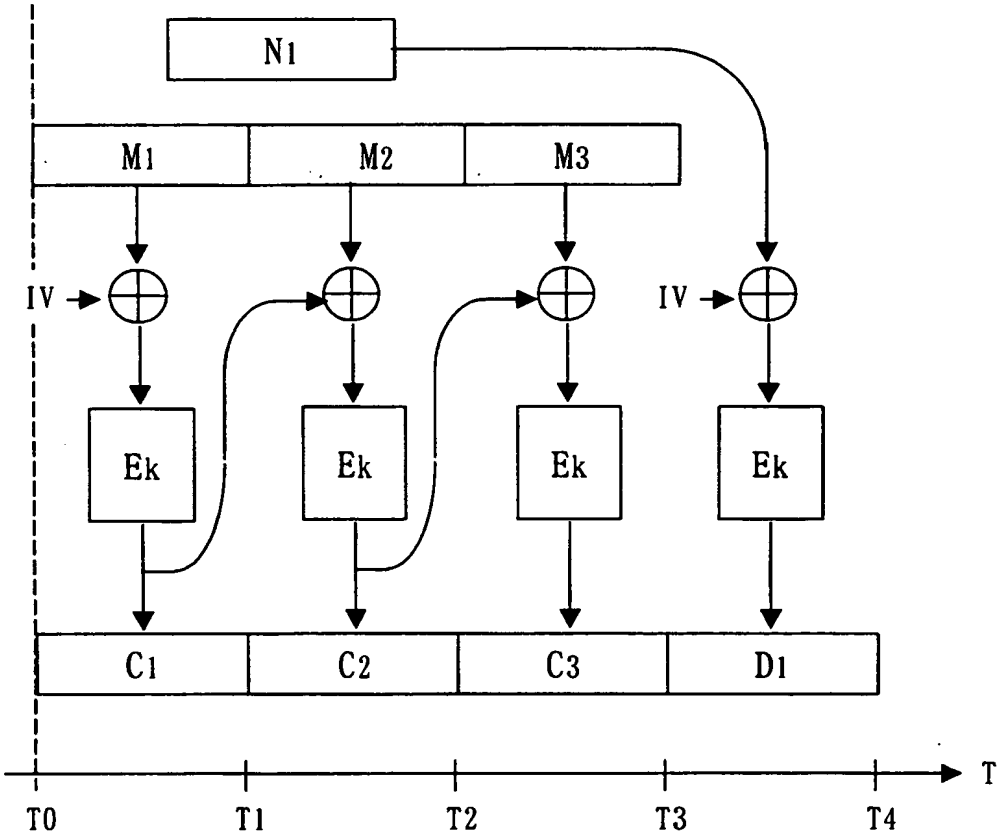


図50

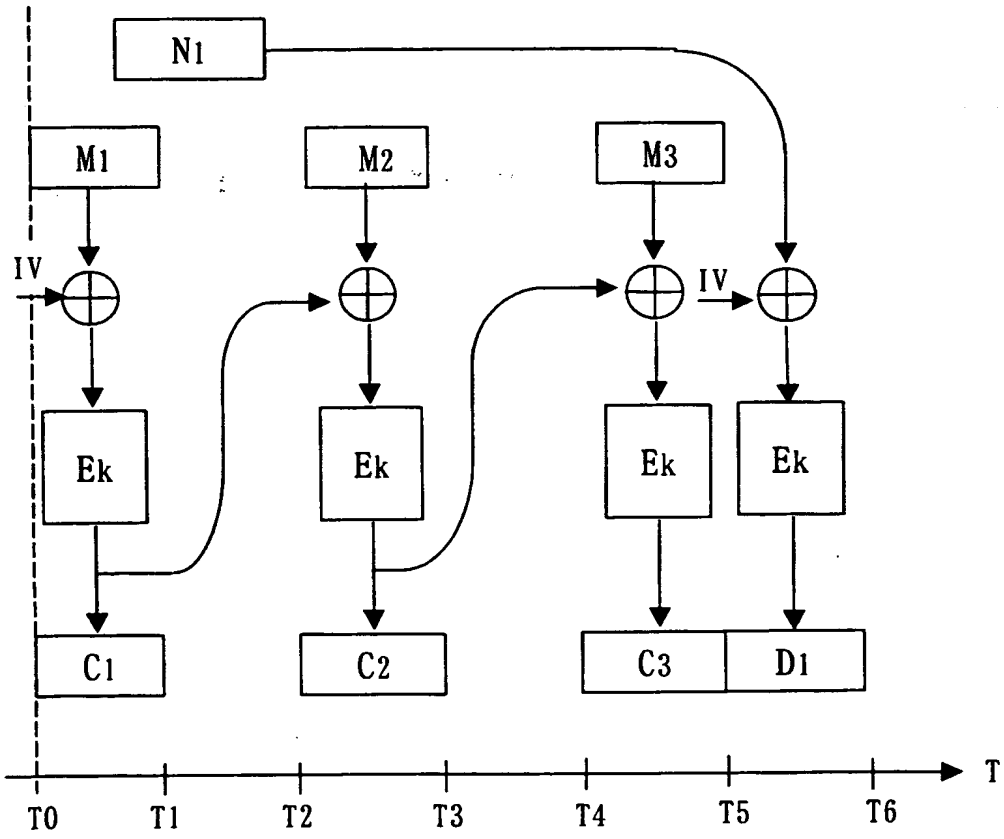


図51

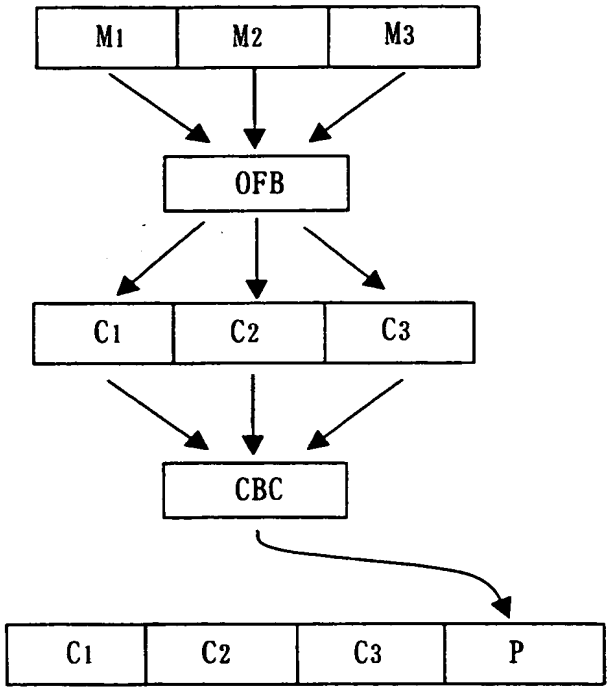
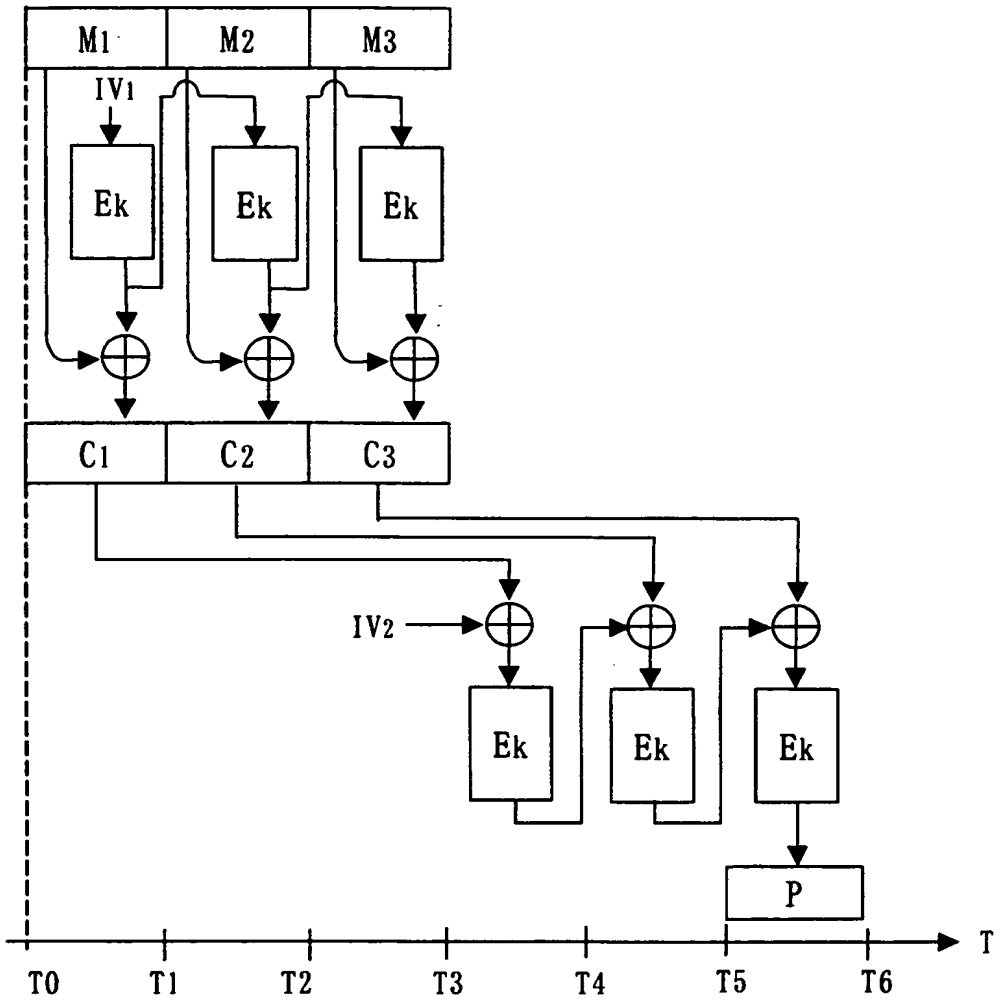


図52



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09129

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04L9/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04L9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP, 9-298736 (Matsushita Electric Ind. Co., Ltd.) 18 November, 1997 (18.11.97) page 10, right column, line 28 to page 12, left column, line 31; all drawings (Family: none)	1-7,11-17, 21-23,27-29, 33,35,37,39, 41-44
X	JP, 10-123950, A (Fuji Xerox Co., Ltd.), 15 May, 1998 (15.05.98), page 4, right column, line 38 to page 5, left column, line 27; Fig. 21	8,10,18,20, 24,26,30,32, 34,36,38,40, 45-50
A	Full text; all drawings & EP, 837383, A2 & US, 6161183, A	9,19,25,31
X	JP, 8-248879, A (International Business Machines Corp.), 27 September, 1996 (27.09.96), page 4, right column, lines 33 to 43; all drawings & EP, 725511, A2 & US, 5673319, A1	8-10,18-20, 24-26,30-32, 34,36,38,40, 45-50

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 March, 2001 (30.03.01)	10 April, 2001 (10.04.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/09129

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 4-48336, A (Fujitsu Limited), 18 February, 1992 (18.02.92), Full text; all drawings (Family: none)	1-50
A	JP, 2-73747, A (NEC Corporation), 13 March, 1990 (13.03.90), Full text; Fig. 1 (Family: none)	1-50
A	JP, 57-69344, A (Nippon Telegr. & Teleph. Corp. <NTT>), 28 April, 1982 (28.04.82), Full text; all drawings (Family: none)	1-50
A	JP, 4-191935, A (Toshiba Corporation), 10 July, 1992 (10.07.92), Full text; all drawings (Family: none)	1-50

国際調査報告

国際出願番号　PCT／JP00／09129

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　H04L9／10

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　H04L9／10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926－1996年
日本国公開実用新案公報	1971－2001年
日本国登録実用新案公報	1994－2001年
日本国実用新案登録公報	1996－2001年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP，9－298736（松下電器産業株式会社） 18．11月．1997（18．11．97） 第10頁右欄第28行目～第12頁左欄第31行目，全図 （ファミリーなし）	1-7, 11-17, 21-23, 27-29, 33, 35, 37, 39, 41-44

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 30．03．01	国際調査報告の発送日 10.04.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木　重徳　印　5W　2956 電話番号　03－3581－1101　内線　3535

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ００／０９１２９

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	ＪＰ，１０－１２３９５０，Ａ（富士ゼロックス株式会社） １５．５月．１９９８（１５．０５．９８） 第４頁右欄第３８行目～第５頁左欄第２７行目，第２１図	8, 10, 18, 20, 24, 26, 30, 32, 34, 36, 38, 40, 45-50
A	全文，全図 ＆　ＥＰ，８３７３８３，Ａ２　＆　ＵＳ，６１６１１８３，Ａ	9, 19, 25, 31
X	ＪＰ，８－２４８８７９，Ａ（インターナショナル・ビジネス・マシーンズ・コーポレイション） ２７．９月．１９９６（２７．０９．９６） 第４頁右欄第３３行目～第４３行目，全図 ＆　ＥＰ，７２５５１１，Ａ２ ＆　ＵＳ，５６７３３１９，Ａ１	8-10, 18-20, 24-26, 30-32, 34, 36, 38, 40, 45-50
A	ＪＰ，４－４８３３６，Ａ（富士通株式会社） １８．２月．１９９２（１８．０２．９２） 全文，全図（ファミリーなし）	1-50
A	ＪＰ，２－７３７４７，Ａ（日本電気株式会社） １３．３月．１９９０（１３．０３．９０） 全文，第１図（ファミリーなし）	1-50
A	ＪＰ，５７－６９３４４，Ａ（日本電信電話公社） ２８．４月．１９８２（２８．０４．８２） 全文，全図（ファミリーなし）	1-50
A	ＪＰ，４－１９１９３５，Ａ（株式会社東芝） １０．７月．１９９２（１０．０７．９２） 全文，全図　（ファミリーなし）	1-50